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

Roles and responsibilities for piloting

Status :	
Dissemination Level :	internal
Work Package :	WP 1
Organisation name of lead partner for this deliverable :	
Author(s):	
Partner(s) contributing :	all WPs

Abstract:
This document contains information about procedures and rules regarding setup and maintenance of an e-CODEX platform.

INTERNAL

History

Version	*Date*	*Changes made*	*Modified by*
0.1	10.07.2013		Anja Prüßmeier Christian Koch
0.4	12.08.2013	Integration of several comments	Anja Prüßmeier
0.5	20.09.2013	Integration of comments from MB	Anja Prüßmeier
0.6	11.10.2013	correction of spelling and grammar	Alexander Weber
0.7	11.03.2014	Adaption for new versions of software components, flow of new platform providers	Tim Nowosatko Anja Prüßmeier
0.8	16.04.2014	Integration of comments from MB	Tim Nowosatko Anja Prüßmeier

INTERNAL

Table of contents

HISTORY **2**
TABLE OF CONTENTS **3**
1. DEFINITIONS AND ABBREVIATIONS **5**
2. SCOPE **6**
3. PARTIES **7**
3.1. E-CODEX WORK PACKAGE 5 (WP5) 7
3.2. E-CODEX WORK PACKAGE 6 (WP6) 7
3.3. E-CODEX WORK PACKAGE 3 (WP3) 7
3.4. E-CODEX WORK PACKAGE 4 (WP4) 7
3.5. E-CODEX PLATFORM PROVIDER 7
3.6. E-CODEX SERVICE PROVIDER 7
3.7. CONTACT POINTS FOR NATIONAL IMPLEMENTATION 8
4. PRECONDITIONS FOR PARTICIPATION IN AN E-CODEX USE CASE **9**
4.1. CIRCLE OF TRUST 9
4.2. QUALITY ASSURANCE 9
4.3. ENVIRONMENTS 10
4.3.1. TEST ENVIRONMENT 10
4.3.2. PRODUCTION ENVIRONMENT 10
5. E-CODEX COMPONENTS **11**
5.1. XML-SCHEMAS 11
5.2. SOFTWARE COMPONENTS AND CONFIGURATION FILES 11
6. COMPONENT DELIVERY **12**
6.1. NAMING OF DELIVERED COMPONENTS 12
6.2. RELEASE DELIVERY AND FORMAT 12
6.2.1. XML-SCHEMAS 12
6.2.2. SOFTWARE COMPONENTS AND RELATED CONFIGURATION FILES 13
6.3. COMPONENT ROADMAP AND RELEASE PLAN 15
6.4. ISSUE MANAGEMENT 16
7. WORKFLOW FOR NEW E-CODEX PLATFORM PROVIDERS **17**
7.1. PILOT PREPARATION 17
7.1.1. REQUEST FOR PILOT 17
7.2. SET UP TEST ENVIRONMENT 18
7.2.1. READY TO TEST 18
7.3. SET UP PRODUCTION ENVIRONMENT 19
7.3.1. FINISH ALL TESTS 19

INTERNAL

7.3.2. PREPARATION FOR GOING LIVE 19
7.3.3. GOING LIVE 20
8. PROBLEM MANAGEMENT & REMEDY 21
8.1. AVAILABILITY 21
9. REFERENCES 22

INTERNAL

1. Definitions and Abbreviations

BSCW	Basic Support for Cooperative Work: Groupware, enabling the sharing of documents.
Bug fix	A Bug fix is a release of software intended to correct bugs in the code, that otherwise would cause malfunctions.
CA	certification authority: an entity that issues digital certificates
CfC	coordination for configuration
DOMIBUS	DOMain Interoperability BUS. Name of the sample implementation of an ebMS 3 message handler done by e-CODEX
ebMS 3	Message Service Specification (ebMS) describes a communication-neutral mechanism Message Service Handlers must implement in order to exchange business documents. ebMS3 is the current version of the specification
keystore	a repository of security certificates
LTS	Long Term Support: A long term supported version of a delivered component will be supported of a specific period of time, normally longer as defined for a normal version of a component.
nightly builds	Nightly builds are software components created automatically each night using the latest revisions of the source files from the code repository
PMode	A *PMode* (Processing Mode) is a concept introduced in the ebMS 3 specification to deal with agreements necessary for successful exchange of data.
sample implementation	A sample implementation is an executable sample software implemented according to a given specification.
XML	Extensible Markup Language
XSD	XML Schema Definition
WP	work package

INTERNAL

2. Scope

The intended readers of this document are implementers and technicians of those countries and platform providers that are participating in e-CODEX piloting or plan to do it.

For the duration of the e-CODEX project the need was identified to give the participants of the piloting phase an overview about:

a) Involved parties

b) Preconditions for participating

c) Planned releases and release timelines

d) Support for releases

e) Handling of Bug fixes

f) Procedures needed for issue management

g) Procedures needed for problem management

INTERNAL

3. Parties

Several organisations within and outside of e-CODEX have to be involved in the process of setting up and operating an e-CODEX piloting environment. The main participants regarding the technical setup are listed here.

3.1. e-CODEX work package 5 (WP5)

One of the technical work packages of e-CODEX, responsible for implementation and building of releases of the e-CODEX software components for the transport layer of e-CODEX (for further information see e-CODEX Technical Annex).

3.2. e-CODEX work package 6 (WP6)

One of the technical work packages of e-CODEX, especially responsible for XML schema development (for further information see e-CODEX Technical Annex).

3.3. e-CODEX work package 3 (WP3)

One of the technical work packages of e-CODEX, responsible for testing and piloting (for further information see e-CODEX Technical Annex).

3.4. e-CODEX work package 4 (WP4)

One of the technical work packages of e-CODEX, responsible for Signatures und Security (for further information see e-CODEX Technical Annex). WP4 does deliver and support an internal software component (security library) which is release integrated into one of the WP5 software components (see Chapter 5.2).

3.5. e-CODEX platform provider

Every entity which has set up and supports an e-CODEX messaging platform and wants to exchange messages in an e-CODEX use case with other e-CODEX messaging platforms. Examples are IT.NRW (hosting the German e-CODEX platform) or the European e-justice portal.

3.6. e-CODEX service provider

Every entity which has set up and supports a software solution in a national context which is connected to the national part (national connector) of the e-CODEX messaging platform (e.g. EGVP in Germany)

INTERNAL

3.7. Contact points for national implementation

One of the preconditions for an e-CODEX platform provider to begin the data exchange is the availability of a signed 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). In chapter 2.2 of this document the parties agreed to appoint Contact Points who shall be responsible for operational and technical matters related to or in connection with the functioning of the e-CODEX System.

The list of contact points will be published on the e-CODEX BSCW server.

INTERNAL

4. Preconditions for participation in an e-CODEX use case

4.1. Circle of trust

One of the preconditions for a party to begin the data exchange in e-CODEX is the availability of a signed 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). This document together with further instructions will be sent to you by WP1.

4.2. Quality Assurance

An e-CODEX platform provider has to undergo a testing phase before it can participate in one of the e-CODEX use cases. These tests consist of:

- A first phase of internal tests by developers
- Integration tests of components (gateway and connector)
- Business tests of national service provider (producing a document and sending it to the national gateway)
- Gateway to gateway tests and connector to connector tests between countries
- End-to-end tests.

For the last two test types, a documentation of the successful execution has to be provided to WP3 by the e-CODEX platform provider in form of a filled in test plan.

A test plan and information about test phases and organisation will be sent out ahead of the testing. As tests are done between two e-CODEX service providers, WP3 will also provide the contact for the partner e-CODEX platform provider to test with. After consulting with the piloting countries, WP3 will also conduct on-site visits for live demonstrations of these tests.

WP3 will evaluate the filled in test plans and decide, collegially with the Management Board and other piloting countries, when the concerned party has attained a satisfactory level of testing to start piloting for the concerned use case (for further information see D3.4).

Each e-CODEX platform provider will have to execute and document tests at the following operations:

- Before the beginning of data exchange in a use case
- After a major release

Each e-CODEX platform provider has to name administrative- and technical coordinators for the pilot phase to WP3, who will be contacted in case of problems or questions during the test phase. These coordinators are also the liaison body to the end-entities in the concerned use case (e.g. the courts)

INTERNAL

4.3. Environments

The test environment as well as the production environment has to be up and running during the whole participation in an e-CODEX pilot phase. To give an overview about the steps a new participant has to undergo during the integration of its e-CODEX platform with their existing platforms a flow diagram has been integrated into Annex I.

Test Environment	Production Environment
Self-signed certificates	CA certified certificates Secure P-Modes storage[1] Two-way SSL authentication

Table 1 – List of security features

4.3.1. Test environment

Each e-CODEX platform provider has to set up and operate a test environment of the e-CODEX platform for at least the duration of the e-CODEX project

WP5 (contact will be named by WP3 see chapter 4.2) has to be informed by each e-CODEX platform provider about the following settings before the intended start of the first data exchange or any intended changes:

- Public key of the used certificates (can be self-signed certificates)
- URL of the gateway
- Supported pilots by MS

WP5 will then issue the necessary configuration files (PModes and keystores) that have to be installed in the test system of the platform provider (for details see section 7.1.1).

4.3.2. Production environment

Each e-CODEX platform provider has to inform WP5 about the following settings at least **four weeks** before the intended start of the first data exchange or any intended changes:

- Public key of the used certificates (should be CA certificates)
- URL of the gateway

WP5 will then issue the necessary configuration files (PModes and keystores) that have to be installed in the production system of the service provider (for details see section 7.3.2)

At least **two weeks before** the intended start of the first data exchange the production environment of the new e-CODEX platform has to be reachable, in order to give the other participants enough time to test configuration and firewall settings.

[1] Secure detached area in the e-CODEX Nexus

INTERNAL

5. E-CODEX Components

The three technical work packages of e-CODEX are responsible for the different components the e-CODEX platform is composed of.

The work packages WP5 and WP6 are responsible for implementation and release of these components. Another component, delivered by WP4, is released integrated into one of the WP5 components. The work package responsible for a component will run tests to prove that the specified technical requirements are met. The results of the tests will be published in the e-CODEX deliverables concerned with testing

5.1. XML-Schemas

After the process modelling of each e-CODEX use case WP6 will create XSDs for each of the business documents required (e.g. forms). Two examples for available XML schemas are:

- European Payment Order
- Small Claims

The schemas as created by WP6 represent the content as agreed upon in Europe, the so called European layer. The deployment of these schemas into automated proceeding in domestic solutions will require mapping between schemas on the European layer and the schemas used in domestic solutions. WP6 has provided several mapping methods out of which participants are free to choose as well as other methods depending on participants preferences. Release planning for the XML schemas is necessary in order to give an e-CODEX platform provider enough time to amend the mapping or if necessary to adjust the national schema, in any kind of release.

5.2. Software components and configuration files

WP5 has provided a sample implementation for the standards for cross-border data exchange defined by e-CODEX which participants are free to implement as well as other implementations depending on participants preferences. The implementation consists of the following software components:

- gateway
- connector framework

Before publishing a release, the functionality of each component will be checked within WP5 by executing the related test plan.

The software component security library (supported by WP4) is integrated into the connector framework.

As the participation in the e-CODEX data-exchange is not limited to those platform providers using the sample implementation, those configuration files of use for other implementations are published separately. These are especially the PMode files (a collection of parameters used in ebMS3 to determine how messages are exchanged between partners) and keystores containing the public keys of the used certificates.

INTERNAL

6. Component delivery

6.1. Naming of delivered components

Version numbers chosen for e-CODEX components will be in the format MAJOR.MINOR.PATCH (e.g. Version 1.3.17). A version will be named by incrementing the name of the prior release according to the following rules:

1. MAJOR version: when introducing major functional changes, especially if they are not backwards-compatible
2. MINOR version: when adding functionality in a backwards-compatible manner, and
3. PATCH version: when making backwards-compatible bug fixes.

Additional labels for long term support, pre-release and build metadata will be named in the MAJOR.MINOR.PATCH format (e.g. Version 2.0.0-SNAPSHOT; Version 1.0.11-LTS).

Version numbers of delivered configuration files will be named in the format MAJOR.NUMBER.ENVIRONMENT (e.g. Version 1.4-prod) according to the following rules:

4. MAJOR: Major version of the associated software component
5. NUMBER: Consecutive number beginning with 1
6. ENVIRONMENT: there will be distinguished between production (prod) and test

Additional labels for further distinction will form extensions to the MAJOR.NUMBER.ENVIRONMENT format.

6.2. Release delivery and format

To inform piloting participants about the technical aspects of releases e-CODEX has set up a mailing list. Every change in release plans and delivered components will be posted through the list (wp3.tech@lists.e-codex.eu). WP3 will integrate participants into the mailing list named to them by the piloting participants.

6.2.1. XML-Schemas

For each use case a set of XSD files will be published by WP6 on the e-CODEX BSCW server[2].

They can be found on the e-CODEX BSCW server. Each release is accompanied by a change log containing the changes between the released and the prior version and compatibility to the prior version.

[2] https://www.jol.nrw.de/bscw/bscw.cgi/2964981

The piloting participants have to agree upon the synchronized exchange of schemas (if needed e.g. in case of major changes) and have to define a planned timeframe for the period of implementation after a new version of a schema has been published.

As the legal valid document is in most Member States not the XML but the PDF-form, a deviation of XML-Versions between the piloting participants would not mean a failure during message transport. The message will be transported even if the mapping of the XML-file would fail due to the use of different schema versions. For e-CODEX service providers (e.g. court applications) this would mean a manual recording from the PDF into the application. Therefore the participants of the e-CODEX piloting will only support one version of the XML-schemas and try to synchronize the exchange of schemas to a set date if needed.

During the piloting phase of e-CODEX, WP3 will provide the means to discuss these issues during their calls and meetings.

6.2.2. Software components and related configuration files

Each release of a software component (see 6.3) is accompanied by a change log, containing the changes between the released and the prior versions and instructions describing the configuration and installation of the released component.

Each release is published on the e-CODEX artefact repository located at https://secure.e-codex.eu/nexus. To access the artefact repository the required user name and password can be found on the e-CODEX BSCW server.

Additionally nightly builds representing the latest state of development can be downloaded from named server. A search for “holodeck-distribution” yields all gateway releases, including nightly builds, identifiable by the SNAPSHOT-tag contained in the version number. Note that the version number does not change between nightly builds, so you have to check the timestamp of the build to identify any updates. Nightly builds are not published on the BSCW server.

Each software component will label one released version as long term supported (LTS). For this version e-CODEX will deliver bug fixes till the next LTS version is released and an additional period of three months. These bug fixes contain no new features nor any support for new use cases. Apart from the version under long term support, only the latest version of each software component will be supported by e-CODEX.

The publication of configuration files is not necessarily linked to the release of a software component. If changes in configuration files are made independently from a release they will be published at least **two weeks before** their intended usage (see chapter 7.3.2), accompanied by a change log. Mandatory exchanges of configuration files will always be linked to a software release.

Piloting platform providers not using the e-CODEX sample implementation have to adapt the changes to their own implementation as deemed necessary by the providers.

INTERNAL

6.2.2.1. Gateway

There are different release packagings available for DOMIBUS, the example implementation done by the e-CODEX project:

Filename: holodeck-distribution-${version}	Gateway WAR-file	Fully configured Tomcat 6 Server	Tomcat server configuration	SQL-scripts for initial database generation (MySQL5, Oracle, Derby)
.war	X			
-distribution-war.zip	X		X	X
-tomcat-full.zip	X	X	X	X
-tomcat-configuration.zip			X	
-sql-scripts.zip				X

Table 2 – Release packaging

and different configuration files:

Environment	Configuration files (pmode, keystores)
Test	X
Production	X

Table 3 – Configuration files

6.2.2.2. Connector framework

Only one packaging of the connector framework is available. Every release of the connector framework will name the releated versions of the gateway it is compatible with.

The security library responsible for signature validation of the business document and signing of a validation report (Trust-OK token), which is delivered by e-CODEX work package 4, is integrated into the connector framework. Configuration files for the connector will be published separately for production and test environment.

It is possible to use the same certificate in the gateway and connector keystore, but during configuration this would mean having to make the configuration changes twice in the different keystores of the separate software components.

INTERNAL

6.3. Component roadmap and release plan

Before the start of the piloting phase and for its duration the e-CODEX project will publish a roadmap for each implemented component on the e-CODEX BSCW server. The roadmap may be consolidated into one document in case of dependencies between the components. The roadmap must contain:

- All planned major component releases
- All planned minor component releases
- Planned new features in the component
- Any incompatibilities between releases of the same or different components
- All planned changes of configuration files (PModes, keystores)
- Information whether the release will be a LTS-version.

Incompatibilities with a prior release will be noted explicitly. Incompatibilities in this context are any change in functionality, interfaces, standards, data formats, etc. introduced in a new release, which break backwards compatibility with a previously released version of the same component, or with an existing and released version of a different component of e-CODEX.

WP5 and WP6 will update their roadmap(s) every half year (six calendar months).

WP5 and WP6 will make available a release plan for each component published on the BSCW-Server. Release plans of more than one component can be made into a consolidated series of one or more documents, for a better overview. The release plan must provide the planned release dates for all maintained software components for at least three months into the future and must include the release dates for

- All major releases
- All minor releases

WP5 and WP6 will inform all named parties whenever the release plan is changed.

In case of incompatibilities of software components, e-CODEX will provide nightly builds of the release candidate(s) of the concerned components including the new feature for at least three months before the official release date.

The directories on the BSCW server where to find the roadmaps and release plans as well as internal rules for work packages can be found in Annex 1.

INTERNAL

6.4. Issue management

For issue and change management in e-CODEX the tool "Jira" is used (for further information see annex 1 of D1.4 Change Management).

For the duration of the e-CODEX project the responsible work package leader will react (acknowledge, that the ticket has been received and take any steps needed for solving the issue) to tickets according to the response times set in below table.

Ticket urgency	Response time
Critical	2 working days
Major	5 working days
Minor	10 working days

Table 4 – Issue Response

Working day

A working day is defined as a normalised day of 8 business hours from 9:00 to 17:00, on five days a week from Monday to Friday, excluding public holidays and regional holidays.

INTERNAL

7. Workflow for new e-CODEX platform providers

The following graphics illustrating the theoretical workflow for new platform providers and is divided into five different states.

Figure 1 – States for pilot preparation

In the following sections, the document will provide a brief overview about all necessary activities for e-CODEX platform providers and also for the official corresponding to the e-CODEX contact points.

All following chapters are in a direct relation to the flowchart in Annex I.

7.1. Pilot Preparation

7.1.1. Request for Pilot

The first step to become a part of the e-CODEX piloting environment is to inform the WP3 coordinator, to get access to the e-CODEX Environment to start testing with other e-CODEX platform providers.

The WP3 coordinator will forward your request to the coordination for configuration (CfC) of e-CODEX, which will provide all necessary information in relation of server configuration, p-Modes[3] (processing Modes) and certificate exchange.

The processing Modes are part of the ebMS 3 concept for message transport between two partner Gateways. The p-Mode concept allows setting up rules for the message transport like Endpoint Address, security configuration and AS4 configuration.

[3] D5.9 Concept of Implementation Chapter 4.6.1.1

To enable the new platform provider to start testing, a set of new configuration files has to be created by the CfC. Therefore the new platform provider has to send the following information to the CfC:

National contact point
Endpoint Address
Gateway Certificate
SSL Certificate (if HTTPS connection configured)
Connector Certificate[4]
Supported pilots

Table 5 - Information for test system

The CFC will create user credentials[5], for the named national contact point of the platform provider and provide the new set of configuration files on the Nexus Repository Server.
After that an information mail will be send to all national contact points, that a new version of configuration files is available and ready for download[6] on the public repository. This version will be automatically recommended for use in all e-CODEX test environments after **7 days**, especially for those platform providers interested in testing with the new participant.

7.2. Set Up Test Environment

7.2.1. Ready to Test

Parallel to providing information for configuration files, a new platform provider should start setting up[7] its test environment.
After downloading the configuration files for your GW version from the Nexus Repository (Pmodes-[Version]-[Timestamp]-test.zip), you should finish the installation during the 7 day time frame for p-Mode update for all GW in the Test Environment. Additional to the Gateway you have to install the MS specific national connector implementation and the necessary truststore, which is also available on Nexus.

A detailed description for setting up a complete e-CODEX Gateway including all necessary configurations can be found in the installation guide provided by WP5.

[4] Public key for security library and Evidence module in connector

[5] User credentials for e-CODEX Nexus

[6] https://secure.e-codex.eu/nexus/content/groups/public/eu/e-codex/pmodes/

[7] https://www.jol.nrw.de/bscw/bscw.cgi/d3610205/Installation%20Instructions.docx

7.3. Set Up Production Environment

7.3.1. Finish all tests

To indicate the successful finish of all tests the documentation of these tests (4.2 Quality Assurance) has to be sent to WP3. At this point the decision is made if the new platform provider is ready to participate within the productive message exchange of e-CODEX.

7.3.2. Preparation for going live

When choosing the DOMIBUS Gateway download[8], install, configure and set up an e-CODEX GW[9] on a separate Server and send all necessary information to the CfC:

National contact point (if differ from Test settings)
Endpoint Address
Gateway Certificate
SSL Certificate (both Client CA and Server Certificate)
Connector Certificate[10]
Supported pilots

Table 6 – Information for production system

The CfC will create user credentials (if they do not already exists) for the named national contact point and provide the new set of configuration files in a secure area[11] of the Nexus Repository Server.
After that an information mail will be send to all productive national contact points that a new version of configuration files is available and ready to download in the secure repository. This version will be automatically recommended for use in all piloting GWs after **2 days**!

Please keep in mind, that all tests in the productive environment can only be done after both testing partners agreed about the test, to be sure that test message will be not be interpreted as productive messages. For this, special messages have to be used instead of test messages from the test environment.

The last requirement to fulfill before going live is to meet the standards of chapter 3 and 5 of the Circle of Trust agreement concerning reliability, data protection and security.

---

[8] https://secure.e-codex.eu/nexus/content/groups/public/org/holodeck/holodeck/

[9] https://www.jol.nrw.de/bscw/bscw.cgi/d3610205/Installation%20Instructions.docx

[10] Public key for security library and Evidence module in connector

[11] Access controlled- Access grant just for the contact points of e-CODEX platform provider and WP3 officials

INTERNAL

7.3.3. Going Live

After the timeframe of 14 days after providing the necessary configuration files, the new platform provider is part of the e-CODEX production system.

INTERNAL

8. Problem management & remedy

The e-CODEX platform provider is responsible for the availability and security of its platform. The requirements for an e-CODEX platform can be found in chapter 3 of the Circle of Trust agreement.

8.1. Availability

To meet the requirements of chapter 3 and Annex 4 of the Circle of Trust agreement, each e-CODEX platform provider will publish information about the measures taken for availability of their e-CODEX platform. As a minimum, information on the following points has to be provided:

- Service hours
- Response times
- Means of contact
- Means of escalation

A template to fill in this information will be published on the e-CODEX BCSW server.

INTERNAL

9. References

The following table lists all references made throughout the document

Reference Nr.	Reference
1	e-CODEX Technical Annex
2	e-CODEX Agreement on a Circle of Trust adopted by the e-CODEX General Assembly on the 20th of February 2013 https://www.jol.nrw.de/bscw/bscw.cgi/3885423
3	Annex 1 of D1.4 Change Management

INTERNAL

I. Appendix

1) WP3: Flow new platform providers

1: Nexus, Mailinglist for technical contacts and generic account for Jira
2: endpoint address, certificate for signing and encryption for test and productive environment
3: minimum 4 weeks before start of piloting
4: minimum 3 weeks before start of piloting