e-CODEX
Agreement on a Circle of Trust

Adopted by the e-CODEX General Assembly on the 20th of February 2013

Definitions

Advanced Electronic Signature	An advanced electronic signature as defined by Article 2 (2) of Directive 1999/93 EC
Advanced Electronic System	An electronic system as outlined in Article 1.2.1.
Authentication-based Advanced Electronic System	A system meeting the requirements set out in Annex 2
Connector	The Connector is a piece of software which implements the interface between (i) the national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal, and (ii) the Gateway of such Party.
Contact Points	Natural and/or legal persons designated by a Party to be responsible for operational and technical matters related to or in connection with the functioning of the e-CODEX System
Document	Any kind of electronic file, such as PDF, XML files, graphics files.
e-CODEX System	The technological and organisational infrastructure, which includes the e-delivery platform (e.g. the e-CODEX Service Provider, the e-CODEX Connector and the e-CODEX Gateway).
Gateway	The technical and organisational infrastructure provided by a Party for incoming and outgoing cross border electronic communication with such Party within the e-CODEX System
Message	An electronic message sent or received by a Gateway via the e-CODEX System, consisting of at least one or

	more Documents, accompanied by a Trust-ok Token.
Original Country of Trust	The state in which the Sending Connector is located that first received the Document, or the state identified by the European E-Justice-Portal.
Party/Parties	The parties to this agreement
Qualified Electronic Signature	An Advanced Electronic Signature based on a qualified certificate and created by a secure signature-creation device, as defined by Article 5 (1) of Directive 1999/93 EC
Receiving State	The state of the Party whose Receiving Gateway receives a Message, or, in the case of the European E-Justice-Portal, the state of the Recipient in each case including the subdivisions and administrative and judicial bodies of that state.
Receiving Party	The Party whose Receiving Gateway receives a Message forwarded from the Sending Gateway via the e-CODEX System
Receiving Connector	The Connector receiving a Message from the Receiving Gateway for forwarding to the Recipient and meeting the requirements set out in Annex 4
Receiving Gateway(s)	The Gateway(s) receiving a Message from the Sending Gateway and meeting the requirements set out in Annex 4
Recipient	The User receiving a Message
Sender	The User indicated as the author of a Message
Sending Party	The Party from whose Sending Gateway a Message is forwarded to the Receiving Gateway(s) via the e-CODEX System
Sending Connector	The Connector first receiving a Message from the sender for forwarding to the Sending Gateway(s) and meeting the requirements set out in Annex 4
Sending Gateway	The Gateway first receiving a Message from the Sending Connector for forwarding to the Receiving Gateway(s) and meeting the requirements set out in Annex 4
Signature-based Advanced Electronic System	An Advanced Electronic System using a Qualified Electronic Signature or an Advanced Electronic

	Signature
Time Evidence	A discrete set of electronic data generated by an electronic system, providing information about the occurrence of a particular event, as further detailed in Annex 5
Trust-ok Token	A software token as described in Article 1.3. and further specified in Annex 3
User	Any party (including courts and public authorities) to a judicial proceeding and/or exchange of information carried out via the e-CODEX System

Preamble: Nature of the Present Agreement

The present Agreement is a document by which the Parties intend to define and establish a Circle of Trust for the cross border 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).

Annex 1[1] lists the Parties who have acceded to this Agreement and in which pilot(s) they are participating.

This preamble forms part of the Present Agreement.

1. Principle of a Circle of Trust

1.1.
For the purpose of this Agreement, the principle of a Circle of Trust is understood as the mutual recognition between Member States of an electronic document within the existing legal framework.

1.2.
In order to fall within the scope of the Circle of Trust, the Document must:

1.2.1.
originate from an Advanced Electronic System, which is an electronic system with the following characteristics:

- The Document is uniquely linked to the User,
- The system is capable of identifying the User,
- The Document is created using means that the User can maintain under his control and any subsequent change of the data is detectable.

[1] Annex 1 will be maintained by the e-CODEX Coordinator.

1.2.2.
be accompanied by a Trust-ok Token issued by the Sending Connector, as described in 1.3. indicating whether the Document is considered as trusted (SUCCESSFUL) or untrusted (UNSUCCESSFUL) in the Original Country of Trust.

1.3.
The characteristics of a Trust-ok Token are specified in Annex 3. In particular, the Trust-ok Token consists of two parts (the token data and the report) as outlined below:

- The content of the report has to be mapped to the content of the token data.
- Based on the content of this report, an assessment must be given about whether or not the document is trusted by the sending party of this Agreement (SUCCESSFUL or UNSUCCESSFUL) in accordance with its policies.

1.4.
There are Signature-based and Authentication-based Advanced Electronic Systems.

- When using a Signature-based Advanced Electronic System the token data must also (i) contain information on whether the signature has been validated successfully, (ii) indicate whether a Qualified Electronic Signature or an Advanced Electronic Signature was applied and (iii) indicate the name of the signatory.

- When using an Authentication-based Advanced Electronic System the token data must also contain information on the identity of the User and on the authentication mechanisms applied by the system.

1.5.
Each Sending Party undertakes to issue a Trust-ok Token for any Document sent via its Sending Gateway.

2. National Contact points

2.1.
The Parties 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.

2.2.
For this purpose, the Parties undertake 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.

3. Reliability and Availability

3.1.
The Sending Connector and the Sending Gateway and the Receiving Gateway and the Receiving Connector must meet the requirements set out in Annex 4.

3.2.
The Parties undertake to set up their Gateways within the e-CODEX System and to 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. Particularly each Party must inform the e-CODEX Coordinator and the other Parties without undue delay about any changes to or incidents at its Connectors, Gateways or Advanced Electronic Systems which lead or have led to a default of their obligations in meeting the requirements set out in this Agreement or which may otherwise have an adverse effect on the reliability of the Circle of Trust.

3.3.
For each Message, each of the Sending Connector and the Receiving Connector shall issue Time Evidences as further detailed in Annex 5 in order to allow the Sender and the Recipient to identify the points of time that are legally relevant.

3.4.
The Parties will agree on measures to avoid risks of system failure.

4. Effects of the Trust-ok Token

Upon receipt of a Message from the Sending Gateway, the Receiving Gateway shall 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.

5. Data Protection and Security Issues

The Parties, through their Contact Points and in compliance with data protection laws at European and national level, shall 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).

Such measures in the application of the criminal pilot should address as a minimum the provisions of Council Framework Decision 2008/977/JHA[2], Art 22 § 2.

6. Amendments

Any amendments to this Agreement (including its Annexes) require the prior approval of the e-CODEX General Assembly.

They enter into force with binding effect for all Parties two months after the approval by the e-CODEX General Assembly. The Parties' right to terminate their participation pursuant to Art. 7 remains unaffected.

However, amendments to Annex 1 do not require the approval of the e-CODEX General Assembly. The e-CODEX Coordinator will, without undue delay, maintain Annex 1 and inform existing Parties of the accession of any new Party or the termination by a Party.

7. Termination

If a Party wants to stop participating in one or more of the pilots it must inform the e-CODEX Coordinator at least one month in advance. Two months after having declared so, the Party will not be bound any more to this Agreement for such pilot(s).

[2] To be replaced by the Directive on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0010:FIN:EN:HTML

Annex 1 to the Agreement on a Circle of trust

List of Parties who have acceded to this Agreement

(This list will be maintained by the Coordinator.)

Annex 2 to the Agreement on a Circle of trust

Authentication-based Advanced Electronic System

An Authentication-based Advanced Electronic System is an electronic system as outlined in Article 1.2.1. of the Agreement (Advanced Electronic System) which meets the following requirements:

Registration
All users have to undergo a registration process requiring identification. For specific roles e.g. lawyers, notaries, the registration process checks with the help of the organisation legally representing this user-group (e.g. national bar association), if the user is really a member of this user-group.

Authenticity
The user is (b) authenticated using an electronic software- certificate plus user-id and password. So the system can (a) uniquely link each created document to the sending user. All documents are created (c) with means, which are under the control of the user (using the own IT-System of the user).

Integrity
The user's system is connected via a Clearing House to the national electronic filing system. A Clearing House has to undergo a certification procedure by or on behalf of or supervised by the Member State's authorities before interconnecting to the National Electronic Legal Communication System (i.e. the national electronic communication system provided by the respective Member State for communication with the courts and linked to the National Connector).
The connections between the user's system and the Clearing House and the connection between the Clearing House and the central components of the National Electronic Legal Communication System are encrypted and secured by electronic certificates. Both the Clearing House and the central components log the whole content of the incoming and outgoing messages at the earliest possible time immediately after receipt resp. before sending. The logs of the Clearing House together with the logs of the Electronic Legal Communication system ensure to follow the trace of any document sent. The logs of the Clearing House and of the central components must be kept at least for 3 months from the date of the message.
Validation modules with extensive checks at the receiving side make sure that only valid applications are received by the courts.
Any subsequent change of a document can be at least manually detected by comparing the messages logged at the sender and receiver side.

Annex 3 to the Agreement on a Circle of trust

Characteristics of the Trust-ok Token

General

The "Trust-OK"-Token will be a PDF-File generated by the sending Connector to provide a human readable document. It contains either the result of the signature and certificate validation or information regarding the authentication process of the user. Additionally, a machine readable form (XML file) will be generated to support future developments.

Content

The token itself will be divided into three parts:

- The first part consists of basic information necessary for the receiving party to recognise documents as trustworthy which includes information on the advanced electronic system and an evaluation of the legal trust level. The legal trust level is stated either as "successful" or "unsuccessful".
- The second part gives a technical assessment of the documents signature (signature-based advanced electronic system) or the authentication information (authentication-based advanced electronic system). This assessment consists of a standardised summary of the original validation data and a technical trust level based on this summary. Furthermore, it displays the results as traffic lights:
  - **For an signature-based advanced electronic system**:
    - Green: The document has been signed with a Qualified or an Advanced Electronic Signature and every necessary validation has been passed.
    - Orange: The document has been signed with a valid Qualified or Advanced Electronic Signature. Within the process of validation, not every service for the validation was accessible, e.g. due to technical problems.
    - Red: The document has not been signed or the signature is invalid.
  - **For an authentication-based advanced electronic system:**
    - Green: The document originates from an authentication-based advanced electronic system, which has authenticated the sender successfully.
    - Red: In any other case.
- The third part will be made of the original validation report provided by either the national solution itself or by the DSS validation tool.

All in all the "Trust OK"-Token will contain:

- Information on the used advanced electronic system
- Information on the time the documents have been filed Basic Information on applied signatures and used certificates or the identity of the user

- Evaluation of the technical trust level (red / orange / green)
- Evaluation of the legal trust level (successful / unsuccessful)
- Original validation report provided by the national solution or the DSS validation tool

Human Readable Token (PDF)

As mentioned above, the human readable token will consist of three parts.

The first part presented on the first page of the actual token includes general information on the advanced electronic system and a legal assessment of the business document. In addition, a national disclaimer and a “validation stamp” showing the legal validation result (successful/unsuccessful) are shown at the bottom of the page.

The second page provides a standardised technical overview of the information from the original validation report -. Depending on the Advanced Electronic System (authentication- or signature-based), the information given by the technical overview varies.

Similar to the first page, the bottom of this page consists of a stamp in the color of the documents technical validation result (green/orange/red) and a short description, e.g. providing additional information about why a document received a orange technical assessment.

The third part of the document consists of the original validation report as it has been created by the issuing member states’ validation software.

Machine Readable Token (XML)

This paragraph provides the XML schema that defines the structure of the XML version of the "Trust Ok"-Token.

```
<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema"
            elementFormDefault="qualified"
            attributeFormDefault="unqualified">

<xsd:element name="TrustOkToken" type="TokenType" />

<xsd: simpleType name="AdvancedSystemEnum">
      <xsd:restriction base=“xsd:string“>
            <xsd:enumeration value="Signature-based" />
            <xsd:enumeration value="Authentication-based" />
      </xsd:restriction>
```

```
</xsd:simpleType>

<xsd:simpleType name="TechnicalTrustLevelEnum">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="FAIL" />
        <xsd:enumeration value="SUFFICIENT" />
        <xsd:enumeration value="SUCCESSFUL" />
    </xsd:restriction>
</xsd:simpleType>

<xsd:simpleType name="LegalTrustLevelEnum">
    <xsd:restriction base="xsd:string">
        <xsd:enumeration value="SUCCESSFUL" />
        <xsd:enumeration value="NOT_SUCCESSFUL" />
    </xsd:restriction>
</xsd:simpleType>

<xsd: complexType name="IssuerType">
    <xsd:sequence>
        <xsd:element name="ServiceProvider" type="xsd:string" />
        <xsd:element name="Country" type="xsd:string" />
        <xsd:element name="AdvancedElectronicSystem" type="“AdvancedSystemEnum“ />
    </ xsd:sequence>
</xsd: complexType>

<xsd:complexType name=" DocumentType">
    <xsd:sequence>
        <xsd:element name="Filename" type="xsd:string" />
        <xsd:element name="Type" type="xsd:string" />
        <xsd:element name="Digest" type="xsd:string" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name=" SourceType ">
    <xsd:sequence>
        <xsd:any minOccurs=“0“ maxOccurs=“unbounded“ />
    </xsd:sequence>
```

```
</xsd: complexType>

<xsd:complexType name="SignatureInformationType">
    <xsd:sequence>
        <xsd:element name="SignatureVerification" type="xsd:boolean" />
        <xsd:element name="StructureVerification" type="xsd:boolean" />
        <xsd:element name="SignatureFormat" type="xsd:string" />
        <xsd:element name="SignatureLevel" type="xsd:string" minOccurs="0" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="CertificateInformationType">
    <xsd:sequence>
        <xsd:element name="Issuer" type="xsd:string" />
        <xsd:element name="CertificateVerification" type="xsd:boolean" />
        <xsd:element name="ValidityAtSigningTime" type="xsd:boolean" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="AuthenticationInformationType">
    <xsd:sequence>
        <xsd:element name="IdentityProvider" type="xsd:string" />
        <xsd:element name="UsernameSynonym" type="xsd:string" />
        <xsd:element name="TimeOfAuthentication" type="xsd:dateTime" />
    </xsd:sequence>
</xsd: complexType>

<xsd:complexType name="SignatureDataType">
    <xsd:sequence>
        <xsd:element name="SigningTime" type="xsd:dateTime" />
        <xs:element name="SignatureInformation" type="SignatureInformationType" />
        <xs:element name="CertificateInformation" type="CertificateInformationType" />
    </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="VerificationDataType">
    <xsd:choice>
```

```
            <xsd:sequence>
                <xsd:element name="SignatureData" type="SignatureDataType"
minOccurs="1" />
                <xsd:element name="AuthenticationData"
type="AuthenticationInformationType" minOccurs="0" />
            </xsd:sequence>
            <xsd:sequence>
                <xsd:element name="SignatureData" type="SignatureDataType"
minOccurs="0" />
                <xsd:element name="AuthenticationData"
type="AuthenticationInformationType" minOccurs="1" />
            </xsd:sequence>
        </xsd:choice>
</xsd:complexType>

<xsd:complexType name="TechnicalResultType">
        <xsd:sequence>
            <xsd:element name="TrustLevel" type="TechnicalTrustLevelEnum" />
            <xsd:element name="Comments" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="LegalResultType">
        <xsd:sequence>
            <xsd:element name="TrustLevel" type="LegalTrustLevelEnum" />
            <xsd:element name="Disclaimer" type="xsd:string" minOccurs="0" />
        </xsd:sequence>
</xsd:complexType>

<xsd:complexType name="ValidationType">
        <xsd:sequence>
            <xs:element name="VerificationTime" type="xsd:dateTime" />
            <xs:element name="VerificationData" type="VerificationDataType" />
            <xs:element name="Result" type="ResultType" />
            <xs:element name="OriginalValidationReport" type="SourceType" />
        </xsd:sequence>
</xsd: complexType>
```

```
<xsd:complexType name="TokenType">
    <xsd:sequence>
        <xsd:element name="Issuer" type="IssuerType" />
        <xsd:element name="Document" type="“DocumentType“ />
        <xsd:element name="Validation" type="“ValidationType“ />
    </xsd:sequence>
</xsd:complexType>

</xsd:schema>
```

Annex 4 to the Agreement on a Circle of trust

Requirements for Connectors

Set up of a Connector

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 (officially accredited trust service provider of the respective state) for signing the ASICS container which is sent from the Connector to the Gateway(s). 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.

Authenticity and Integrity

The Receiving Connector has to process the document(s) and the Trust-ok Token in accordance with the laws of the Receiving State.

Only authorized and authenticated persons (by means of a strong and properly administered user-Id and password) must have access to the Connector.

The operating authority of a Connector must monitor the performance of their Connector as established by their normal business hours. In case of any failure the operating authority must put into place measures to address this failure as fast as is reasonably possible.

Requirements for Gateways

Set up of a Gateway

An e-CODEX 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 2 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 published via http://joinup.ec.europa.eu/. 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

The exchange of Messages and other information between the Gateways has to be done encrypted by SSL encryption. An e-CODEX 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 authorized and authenticated persons (by means of a strong and properly administered user-Id and password) must have access to the Gateway.

The operating authority of a Gateway must monitor performance of their Connector as established by their normal business hours. In case of any failure the operating authority must put into place measures to address this failure as fast as is reasonably possible.

<u>Annex 5 to the Agreement on a Circle of trust</u>

List of Time Evidences

- The description of the time evidences may include:
  - **What** XML, PDF, or any other electronic support of the time evidence
  - **Why** the fact that triggers the time evidence production
  - **When** the moment or step of the process at which the time evidence is generated
  - **Where** the point in which the time evidence is created (system, application…)
  - **Who** electronic (or even human) actor accountable for the time evidence
  - **How** a short explanation of the way the time evidence is produced
- e-CODEX time evidences are generated by the Sending or Receiving Connector (in particular by the EvidenceBuilder) based on the ETSI REM standard

List of time evidences

Details given in this list are: 🗎 the name of the evidence in the technical workflow; detail description in form of What, Why, When, Where, Who and How; what happen if the evidence is positive ☑ or negative ☒.

🗎 **Submission Evidence** // SubmissionAcceptanceRejection()

- **What** REM ETSI evidence
- **Why** the Message has been successfully processed (transformation, AsicsContainer and TrustOkToken) in order to be sent by the Sending Connector
- **When** a Message is first received by the Sending Connector
- **Where** EvidenceBuilder module of the Sending Connector
- **Who** Owner of the Sending Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [SubmissionAcceptance] It is (1) added to the Message to be submitted from the Sending Connector to the Sending Gateway and (2) sent to the Sender after the Message has been submitted to the Sending Gateway

☒ [SubmissionRejection] If there is an error it is only sent to the Sender immediately.

RelayREMMD Evidence // RelayREMMDAcceptanceRejection ()

- **What** REM ETSI evidence
- **Why** the Message has arrived at the Receiving Gateway (and Connector)
- **When** the Message has been received by the Receiving Connector
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [RelayREMMD Acceptance] confirm the arrival of the Message in the Receiving Connector

☒ [RelayREMMD Rejection] The Sending Connector starts a timer at the moment of sending the message. If the period of time expired without receiving a RelayREMMD Acceptance from the Receiving Connector, a Relay REMMD Rejection is generated.

Delivery Evidence // DeliveryNonDeliveryToRecipient ()

- **What** REM ETSI evidence
- **Why** the Message has been delivered to the Recipient's mailbox
- **When** after the Message has arrived in the Recipient's mailbox and corresponding evidence from the national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal (in each case if available) has been received.
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [deliveryEvidence Acceptance] the Message has been successfully delivered to the Recipient's mailbox

☒ [deliveryEvidence Rejection] the Message delivery to the Recipient's mailbox has not been achieved

Retrieval Evidence // RetrievalNonRetrievalToRecipient ()

- **What** REM ETSI evidence
- **Why** the the Recipient's national e-justice communication infrastructure designated to process Documents within the scope of activities of the respective Party or, in the case of the European Commission, the European E-Justice Portal, communicates to the Receiving Connector that the Recipient has successfully retrieved – according to the applicable national rules – the message to the Recipient. This is when the Recipient really opens his mailbox.
- **When** according to the applicable national rules
- **Where** EvidenceBuilder module of the Receiving Connector
- **Who** Owner of the Receiving Connector (usually the MoJ of the Member State)
- **How** According to REM ETSI standards

☑ [retrievalEvidence Acceptance] the Recipient has successfully retrieved the Message.

☒ [retrievalEvidence Rejection] the Recipient has not been able to retrieve the Message

Declaration of Accession:

The subscribing e-CODEX partner hereby declares to the e-CODEX Coordinator that he complies with the terms of this Agreement and its annexes for his e-CODEX piloting activities.

Name of legal entity: _____
(full name of the e-CODEX partner)

Name of legally authorised representative: _____
(written out in full)

Title of legally authorised representative: _____

Signature of legally authorised representative: _____

Place: _____ Date: _____

Stamp of the organisation: