Gesetz- und Verordnungsblatt

FÜR DAS LAND NORDRHEIN-WESTFALEN

69. Jahrgang	Ausgegeben zu Düsseldorf am 10. April 2015	Nummer 17

45

Verordnung über die elektronische Kommunikation und Aktenführung in Angelegenheiten der strafrechtlichen Zusammenarbeit mit dem Ausland im Lande Nordrhein-Westfalen (ERVVO RHSt)

Vom 24. März 2015

Auf Grund des § 77b des Gesetzes über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), der durch Artikel 1 des Gesetzes vom 18. Oktober 2010 (BGBl. I S. 1408) eingefügt worden ist, in Verbindung mit § 1 Absatz 2 des Justizgesetzes Nordrhein-Westfalen vom 26. Januar 2010 (GV. NRW. S. 30) verordnet das Justizministerium:

§ 1
Zulassung der elektronischen Kommunikation im Bereich der Rechtshilfe in Strafsachen

Gerichte und Behörden können nach Maßgabe der nachfolgenden Vorschriften elektronische Nachrichten zum Zweck der internationalen Rechtshilfe in Strafsachen von ausländischen Gerichten und Behörden empfangen oder an diese senden. Die an dem elektronischen Nachrichtenverkehr teilnehmenden in- und ausländischen Behörden sowie der Zeitpunkt, ab dem sie daran teilnehmen, sind in **Anlage 1** bezeichnet.

§ 2
Arten und Formate der zu übermittelnden Dokumente

(1) Nachrichten nach § 1 bestehen aus einem Hauptdokument und maschinenlesbaren Daten im Format XML (Extensible Markup Language). Die Beifügung von Anlagen zu einem Hauptdokument (Anhänge) ist zulässig.

(2) Das Hauptdokument enthält das an die empfangende Behörde zu übermittelnde Anschreiben das Rechtshilfeersuchen betreffend im Format Adobe PDF (Portable Document Format). Ein Anhang soll eines der folgenden Formate aufweisen:

1. ASCII (American Standard Code for Information Interchange) ohne Formatierungscodes oder Sonderzeichen,
2. Unicode,
3. Microsoft RTF (Rich Text Format),
4. Adobe PDF (Portable Document Format),
5. TIFF (Tag Image File Format),
6. JPEG (Image-Format),
7. Microsoft XLS (Exel Format),
8. HTML (Text-Format),
9. Microsoft Word ohne aktive Komponenten.

(3) Elektronische Dokumente, die einem der in Absatz 2 genannten Dateiformate entsprechen, dürfen in komprimierter Form im Format ZIP übermittelt werden. Eine komprimierte Datei darf keine komprimierten Dateien und keine Verzeichnisstrukturen enthalten. Beim Einsatz von Dokumentensignaturen muss sich die Signatur auf das Dokument und nicht auf die komprimierte Datei beziehen.

(4) XML-Dateien sollen im UNICODE-Zeichensatz UTF-8 codiert sein.

(5) Die übermittelnde Behörde ist dafür verantwortlich, dass die Nachricht selbst und die angehängten Dateien keine schädlichen aktiven Komponenten wie beispielsweise Viren, Trojaner oder Würmer enthalten.

§ 3
Innerstaatliche Übermittlung von Nachrichten

Die Übermittlung elektronischer Nachrichten nach § 1 von und an die zuständigen Gerichte und Behörden erfolgt auf nordrhein-westfälischer Seite durch die Anwendung Elektronisches Gerichts- und Verwaltungspostfach (EGVP) an die in der Anlage 1 bezeichnete nationale Empfangseinrichtung (e-Codex-Gateway).

§ 4
Datenverarbeitung zur Nachrichtenübermittlung zwecks elektronischer Umwandlung (Mapping)

Zum Zwecke der Umschreibung maschinenlesbarer Daten aus und in eine den Organisatorisch-technischen Leitlinien für den elektronischen Rechtsverkehr mit den Gerichten und Staatsanwaltschaften der Bund-Länder Arbeitsgruppe Elektronischer Rechtsverkehr vom 21.4. 2005 (OT-Leit-ERV) entsprechenden Form (Mapping) darf der in der Anlage 1 bezeichnete nationale Betreiber der nationalen Empfangseinrichtung (e-Codex-Gateway) Nachrichten verarbeiten, soweit dies für die Nachrichtenübermittlung erforderlich ist. Zu diesem Zweck können personenbezogene Daten vorübergehend gespeichert werden, eine dauerhafte Speicherung ist jedoch nicht zulässig.

§ 5
Gewährleistung der Authentizität von an das Ausland zu übermittelnden Hauptdokumenten und der Integrität von zu übermittelnden Hauptdokumenten und Nachrichten

(1) Eine Mehrfertigung des Hauptdokuments ist durch die in Nummer 9 Absatz 1 der Richtlinien über den Verkehr mit dem Ausland in Strafsachen vom 5. Dezember 2012 (BAnz 2012, AT 19.12.2012 B2) bezeichnete Person zu unterzeichnen. Die unterzeichnete Mehrfertigung ist zu den Akten zu nehmen. Das Hauptdokument ist elektronisch im Format PDF zu speichern und mit einer fortgeschrittenen elektronischen Signatur zu versehen.

(2) Dem Hauptdokument beizufügende Anhänge sind durch Einscannen in die elektronische Form zu übertragen. Ist ein beizufügendes Schriftstück mit einem Beglaubigungsvermerk versehen, so ist im Hauptdokument die bildliche und inhaltliche Übereinstimmung des auf dem beigefügten Schriftstück angebrachten Beglaubigungsvermerks zu bestätigen.

(3) Abweichend von Nummer 9 Absatz 3 der Richtlinien über den Verkehr mit dem Ausland in Strafsachen bedarf es der Beifügung eines Dienstsiegels nicht.

(4) Der Betreiber der nationalen Empfangseinrichtung gewährleistet bei der Weiterleitung der Nachricht an das Ausland die Integrität der an das Ausland zu übermittelnden Nachrichten entsprechend den international anerkannten Standards.

§ 6
Prüfung der Authentizität und Integrität von aus dem Ausland übermittelten Dokumenten und Nachrichten

(1) Sofern nach dem Gesetz über die internationale Rechtshilfe in Strafsachen in der Fassung der Bekanntmachung vom 27. Juni 1994 (BGBl. I S. 1537), das zuletzt durch Artikel 4 des Gesetzes vom 8. Juli 2014 (BGBl. I S. 890) geändert worden ist, für die Leistung von Rechtshilfe die Einreichung schriftlicher Unterlagen einschließlich von Originalen oder beglaubigten Abschriften vorgesehen ist, ist die Vorlage elektronischer Dokumente zulässig, die mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876) in der jeweils geltenden Fassung versehen sind. Die qualifizierte elektronische Signatur kann durch ein anderes sicheres Verfahren ersetzt werden, das die Authentizität und die Integrität eines übermittelten elektronischen Dokuments sicherstellt (§ 77a Absatz 2 des Gesetzes über die internationale Rechtshilfe in Strafsachen).

(2) Als anderes sicheres Verfahren im Sinne des § 77a Absatz 2 des Gesetzes über die internationale Rechtshilfe in Strafsachen, das die empfangende Stelle von der Prüfung der Authentizität des übermittelten elektronischen Dokuments und der Integrität der übermittelten Nachricht durch den übermittelnden ausländischen Staat entbindet, gilt auch die Bestätigung durch die Beifügung eines „Trust-OK-Token“ nach Maßgabe des sich aus **Anlage 2** ergebenden europäischen Standards.

(3) Sofern eine qualifizierte elektronische Signatur nach § 2 Nummer 3 des Signaturgesetzes verwendet wird, muss diese und das ihr zugrunde liegende Zertifikat durch das adressierte Gericht oder durch eine andere von der Landesjustizverwaltung mit der automatisierten Überprüfung beauftragte Stelle prüfbar sein.

(4) Die eingereichten Schriftstücke müssen für die Bearbeitung durch ein Gericht oder eine Behörde geeignet sein. Ist ein übermitteltes elektronisches Dokument zur Bearbeitung nicht geeignet, ist dies dem Absender unter Angabe der geltenden technischen Rahmenbedingungen unverzüglich mitzuteilen.

§ 7
Weitere Bearbeitung eingehender elektronischer Nachrichten aus dem Ausland

Soweit nicht die elektronische Aktenführung zugelassen ist, ist von eingehenden elektronischen Dokumenten, sofern es sich nicht um maschinenlesbare Dateien handelt, ein Aktenauszug zu fertigen. Im Übrigen bleiben die Vorschriften der Anweisungen für die Verwaltung des Schriftguts bei den Geschäftsstellen der Gerichte und Staatsanwaltschaften des Landes Nordrhein-Westfalen – AV des Justizministeriums vom 27. April 1967 (JMBl. NRW S. 109) – die zuletzt durch AV vom 29. November 2013 (JMBl. NRW S. 321) geändert worden ist – unberührt.

§ 8
Inkrafttreten

Diese Verordnung tritt am Tage nach der Verkündung in Kraft.

Düsseldorf, den 24. März 2015

Der Justizminister
des Landes Nordrhein-Westfalen
Thomas K u t s c h a t y

Anlage 1
zur Verordnung über die elektronische Kommunikation und Aktenführung in Angelegenheiten der strafrechtlichen Zusammenarbeit mit dem Ausland im Lande Nordrhein-Westfalen vom 24. März 2015

I. Am elektronischen Rechtshilfeverkehr in Strafsachen teilnehmende Gerichte und Behörden, Zeitpunkt der Teilnahme

Staatsanwaltschaften	**Zeitpunkt**
Aachen, Düsseldorf	ab 01.02.2015
Duisburg, Krefeld, Kleve, Köln, Mönchengladbach	ab 01.09.2015
Arnsberg, Bielefeld, Bochum, Bonn, Detmold, Dortmund, Essen, Hagen, Münster, Paderborn, Siegen, Wuppertal	ab 01.12.2015

II. Nationale Empfangseinrichtung (e-Codex-Gateway)

Landesbetrieb
Information und Technik Nordrhein-Westfalen (IT.NRW)
Mauerstraße 51
40476 Düsseldorf

Anlage 2
zur Verordnung über die elektronische Kommunikation und Aktenführung in Angelegenheiten der strafrechtlichen Zusammenarbeit mit dem Ausland im Lande Nordrhein-Westfalen vom 24. März 2015

e-CODEX making justice faster.eu

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

e CODEX making justice faster.eu

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.)

e CODEX making justice faster.eu

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.

e-CODEX making justice faster.eu

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>
```

e-CODEX making justice faster.eu

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.

e-CODEX making justice faster.eu

Annex 5 to the Agreement on a Circle of trust

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

e-CODEX making justice faster.eu

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:

600

Dritte Verordnung zur Änderung der Finanzamtszuständigkeitsverordnung

Vom 25. März 2015

Auf Grund

1. des § 17 Absatz 1 des Finanzverwaltungsgesetzes in der Fassung der Bekanntmachung vom 4. April 2006 (BGBl. I S. 846, 1202),
2. des § 17 Absatz 2 Satz 3 des Finanzverwaltungsgesetzes in der Fassung der Bekanntmachung vom 4. April 2006 (BGBl. I S. 846, 1202),
3. des § 387 Absatz 2 Satz 1 und 2 und des § 409 Satz 2 der Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866; 2003 I S. 61),
4. des § 14 Absatz 3 Satz 2 des Fünften Vermögensbildungsgesetzes in der Fassung der Bekanntmachung vom 4. März 1994 (BGBl. I S. 406),
5. des § 8 Absatz 2 Satz 2 des Wohnungsbau-Prämiengesetzes in der Fassung der Bekanntmachung vom 30. Oktober 1997 (BGBl. I S. 2678),
6. des § 29a Absatz 2 des Berlinförderungsgesetzes in der Fassung der Bekanntmachung vom 2. Februar 1990 (BGBl. I S. 173),
7. des § 20 des Berlinförderungsgesetzes in der Fassung der Bekanntmachung vom 2. Februar 1990 (BGBl. I S. 173),
8. es § 9 des Investitionszulagengesetzes 1996 in der Fassung der Bekanntmachung vom 22. Januar 1996 (BGBl. I S. 60),
9. des § 8 des Investitionszulagengesetzes 1999 in der Fassung der Bekanntmachung vom 11. Oktober 2002 (BGBl. I S. 4034),
10. des § 7 des Investitionszulagengesetzes 2005 in der Fassung der Bekanntmachung vom 30. September 2005 (BGBl. I S. 2961),
11. des § 14 des Investitionszulagengesetzes 2007 in der Fassung der Bekanntmachung vom 23. Februar 2007 (BGBl. I S. 282),
12. des § 15 des Investitionszulagengesetzes 2010 vom 7. Dezember 2008 (BGBl. I S. 2350),
13. des § 6 des Stahlinvestitionszulagengesetzes vom 22. Dezember 1981 (BGBl. I S. 1523, 1557),
14. des § 164 Satz 1 des Steuerberatungsgesetzes in der Fassung der Bekanntmachung vom 4. November 1975 (BGBl. I S. 2735), der durch Artikel 9 Nummer 5 des Gesetzes vom 18. August 1980 (BGBl. I S. 1537) geändert worden ist,
15. des § 17 Absatz 4 des Geldwäschegesetzes vom 13. August 2008 (BGBl. I S. 1690), der durch Artikel 1 Nummer 19 Buchstabe c und d des Gesetzes vom 22. Dezember 2011 (BGBl. I S. 2959) geändert worden ist,
16. des § 131 Absatz 3 des Gesetzes über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602),

zu Nummer 4 bis 6 jeweils in Verbindung mit § 387 Absatz 2 Satz 1 und 2 sowie § 409 Satz 2 der Abgabenordnung in der Fassung der Bekanntmachung vom 1. Oktober 2002 (BGBl. I S. 3866, 2003 I S. 61), zu Nummer 7 bis 15 jeweils in Verbindung mit § 387 Absatz 2 Satz 1 und 2 der Abgabenordnung, zu Nummer 16 in Verbindung mit § 409 Satz 2 der Abgabenordnung und zu Nummer 2 bis 14 und Nummer 16 jeweils in Verbindung mit § 1 der Delegationsverordnung FM vom 23. April 2013 (GV. NRW. S. 198),

verordnet das Finanzministerium:

Artikel 1

Die Finanzamtszuständigkeitsverordnung vom 17. Juni 2013 (GV. NRW. S. 350), die zuletzt durch Verordnung vom 5. Juni 2014 (GV. NRW. S. 325) geändert worden ist, wird wie folgt geändert:

1. In der Inhaltsübersicht wird die Angabe zu § 6 wie folgt gefasst:

   „§ 6 Liquiditätsprüfung“.

2. § 2 Absatz 3 wird wie folgt geändert:

   a) Nummer 19 wird wie folgt gefasst:

      „19. der Bezirks des Finanzamts Gelsenkirchen mit Sitz in Gelsenkirchen
      die Stadt Gelsenkirchen,“

   b) Nummer 20 wird aufgehoben.

   c) Die Nummern 21 bis 50 werden die Nummern 20 bis 49.

3. § 5 Nummer 3 wird wie folgt geändert:

   a) In Buchstabe c wird das Komma am Ende durch einen Punkt ersetzt.

   b) Buchstabe d wird aufgehoben.

4. Nach § 5 wird folgender § 6 eingefügt:

   „§ 6
   Liquiditätsprüfung

   Für die Durchführung von Liquiditätsprüfungen sind abweichend von der Bezirksgliederung nach § 2 zuständig

   1. im Oberfinanzbezirk Köln der Oberfinanzdirektion Nordrhein-Westfalen
      das **Finanzamt Bergisch Gladbach**
      zusätzlich für die Bezirke der Finanzämter Köln-Altstadt und Köln-Mitte , Köln-Nord, Köln-Ost, Köln-Porz, Köln-Süd, Köln-West und Leverkusen;
   2. im Oberfinanzbezirk Münster der Oberfinanzdirektion Nordrhein-Westfalen
      das **Finanzamt Detmold**
      zusätzlich für die Bezirke der Finanzämter Gütersloh, Höxter, Lemgo, Paderborn, Warburg und Wiedenbrück.“

5. Die Fußnote zu § 6 wird aufgehoben.

6. In § 3 Absatz 1 Nummer 3 Buchstabe a, § 4 Nummer 3 Buchstabe b, § 7 Absatz 1 Nummer 3 Buchstabe b, § 19 Nummer 3 Buchstabe b, § 22 Satz 1 Buchstabe e, § 23 Nummer 3 Buchstabe e und f und § 24 Nummer 3 Buchstabe b werden jeweils die Wörter „Gelsenkirchen-Nord, Gelsenkirchen-Süd“ durch das Wort „Gelsenkirchen“ ersetzt.

Artikel 2

Diese Verordnung tritt am 1. Mai 2015 in Kraft.

Düsseldorf, den 25. März 2015

Der Finanzminister
des Landes Nordrhein-Westfalen
Dr. Norbert W a l t e r - B o r j a n s

– GV. NRW. 2015 S. 349

1. Änderung des Regionalplans für den Regierungsbezirk Arnsberg, Teilabschnitt Oberbereich Siegen (Kreis Siegen-Wittgenstein und Kreis Olpe), im Gebiet der Stadt Freudenberg

Vom 30. März 2015

Der Regionalrat des Regierungsbezirks Arnsberg hat in seiner Sitzung am 3. Dezember 2014 die 1. Änderung des Regionalplans für den Regierungsbezirk Arnsberg, Teilabschnitt Oberbereich Siegen (Kreis Siegen-Wittgenstein und Kreis Olpe), Erweiterung eines Bereiches für gewerbliche und industrielle Nutzungen, im Gebiet der Stadt Freudenberg aufgestellt.

Diese Änderung hat mir die Regionalplanungsbehörde Arnsberg mit Bericht vom 11. Dezember 2014 – Aktenzeichen: 32.1.2.1./10.4 – 1. Änd. – gemäß § 19 Absatz 6 des Landesplanungsgesetzes NRW vom 3. Mai 2005 (GV. NRW. S. 430), zuletzt geändert durch Artikel 2 des Gesetzes vom 29. Januar 2013 (GV. NRW. S. 33), angezeigt.

Die Bekanntmachung im Gesetz- und Verordnungsblatt für das Land Nordrhein-Westfalen erfolgt nach § 14 Satz 1 Landesplanungsgesetz NRW.

Gemäß § 14 Satz 3 Landesplanungsgesetz NRW wird die Änderung des Regionalplans bei der Staatskanzlei des Landes Nordrhein-Westfalen (Landesplanungsbehörde), der Bezirksregierung Arnsberg (Regionalplanungsbehörde) sowie dem Kreis Siegen-Wittgenstein und der Stadt Freudenberg zur Einsicht für jedermann niedergelegt.

Die Änderung des Regionalplans wird mit der Bekanntmachung wirksam (§ 14 Satz 2 Landesplanungsgesetz NRW). Damit sind die Ziele gemäß §§ 4 und 5 Raumordnungsgesetz vom 22. Dezember 2008 (BGBl. I S. 2986), das zuletzt durch Artikel 9 des Gesetzes vom 31. Juli 2009 (BGBl. I S. 2585) geändert worden ist, zu beachten.

Ich weise darauf hin, dass die in § 15 Landesplanungsgesetz NRW in Verbindung mit § 12 Absatz 5 Raumordnungsgesetz genannte Verletzung von Verfahrens- und Formvorschriften und von Mängeln der Abwägung bei der Erarbeitung und Aufstellung der Änderung des Regionalplanes unbeachtlich werden, wenn sie nicht innerhalb eines Jahres seit Bekanntmachung des Regionalplans gegenüber der Bezirksregierung Arnsberg (Regionalplanungsbehörde) unter Darlegung des die Verletzung begründenden Sachverhalts geltend gemacht worden ist.

Düsseldorf, den 30. März 2015

Die Ministerpräsidentin
des Landes Nordrhein-Westfalen

Im Auftrag

Dr. Christoph E p p i n g

– GV. NRW. 2015 S. 349

Einzelpreis dieser Nummer 5,40 Euro
zuzügl. Porto- und Versandkosten

Bestellungen, Anfragen usw. sind an den A. Bagel Verlag zu richten. Anschrift und Telefonnummer wie folgt für
Abonnementsbestellungen: Grafenberger Allee 82, Fax (02 11) 96 82/2 29, Tel. (02 11) 96 82/2 38 (8.00–12.30 Uhr), 40237 Düsseldorf
Bezugspreis halbjährlich 33,50 Euro (Kalenderhalbjahr). Jahresbezug 67,– Euro (Kalenderjahr), zahlbar im Voraus. Abbestellungen für Kalenderhalbjahresbezug müssen bis zum 30. 4. bzw. 31. 10., für Kalenderjahresbezug bis zum 31. 10. eines jeden Jahres beim A. Bagel Verlag vorliegen.
Reklamationen über nicht erfolgte Lieferungen aus dem Abonnement werden nur innerhalb einer Frist von vier Wochen nach Erscheinen anerkannt.

In den Bezugs- und Einzelpreisen ist keine Umsatzsteuer i. S. d. § 14 UStG enthalten.

Einzelbestellungen: Grafenberger Allee 82, Fax (02 11) 96 82/2 29, Tel. (02 11) 96 82/2 41, 40237 Düsseldorf
Von Vorabeinsendungen des Rechnungsbetrages – in welcher Form auch immer – bitten wir abzusehen. Die Lieferungen erfolgen nur auf Grund schriftlicher Bestellung gegen Rechnung. Es wird dringend empfohlen, Nachbestellungen des Gesetz- und Verordnungsblattes für das Land Nordrhein-Westfalen möglichst innerhalb eines Vierteljahres nach Erscheinen der jeweiligen Nummer beim A. Bagel Verlag vorzunehmen, um späteren Lieferschwierigkeiten vorzubeugen. Wenn nicht innerhalb von vier Wochen eine Lieferung erfolgt, gilt die Nummer als vergriffen. Eine besondere Benachrichtigung ergeht nicht.
Herausgeber: Landesregierung Nordrhein-Westfalen, Haroldstraße 5, 40213 Düsseldorf
Herstellung und Vertrieb im Namen und für Rechnung des Herausgebers: A. Bagel Verlag, Grafenberger Allee 82, 40237 Düsseldorf
Druck: TSB Tiefdruck Schwann-Bagel, Düsseldorf und Mönchengladbach
ISSN 0177-5359