DECISIÓN DE EJECUCIÓN (UE) 2022/2519 DE LA COMISIÓN

de 20 de diciembre de 2022

relativa a las normas y especificaciones técnicas del sistema e-CODEX, incluidas las relativas a la seguridad y a los métodos de verificación de la integridad y la autenticidad

(Texto pertinente a efectos del EEE)

LA COMISIÓN EUROPEA,

Visto el Tratado de Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726 ([1]), y en particular su artículo 6, apartado 1, letra a),

Considerando lo siguiente:

(1) De conformidad con el artículo 5 del Reglamento (UE) 2022/850, el sistema e-CODEX está compuesto por un punto de acceso e-CODEX, unas especificaciones de procesamiento digital y los productos de soporte lógico (*software*), la documentación y otros recursos de apoyo enumerados en el anexo de dicho Reglamento.

(2) El punto de acceso e-CODEX se compone de una pasarela que consta de un soporte lógico (*software*), basado en un conjunto común de protocolos, que posibilita el intercambio seguro de información a través de una red de telecomunicaciones con otras pasarelas que utilizan el mismo conjunto común de protocolos, y de un conector que permite vincular los sistemas conectados con la pasarela y consta de un soporte lógico (*software*) basado en un conjunto común de protocolos abiertos.

(3) A fin de garantizar que el proceso para el traspaso del sistema e-CODEX y la asunción de su control por parte de eu-LISA sea satisfactorio y permitir a la agencia desempeñar las tareas que se le encomiendan, deben establecerse las normas y especificaciones técnicas mínimas, incluidas las relativas a la seguridad y los métodos de verificación de la integridad y la autenticidad, en las que se sustentan los componentes del sistema e-CODEX.

(4) De conformidad con los artículos 1 y 2 del Protocolo n.º 22 sobre la posición de Dinamarca, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, Dinamarca no participó en la adopción del Reglamento (UE) 2022/850 y, por consiguiente, no está vinculada por la presente Decisión ni sujeta a su aplicación.

(5) De conformidad con los artículos 1 y 2 y el artículo 4 *bis*, apartado 1, del Protocolo n.º 21 sobre la posición del Reino Unido y de Irlanda respecto del espacio de libertad, seguridad y justicia, anejo al Tratado de la Unión Europea y al Tratado de Funcionamiento de la Unión Europea, y sin perjuicio del artículo 4 de dicho Protocolo, Irlanda no participó en la adopción del Reglamento (UE) 2022/850 y, por consiguiente, no está vinculada por la presente Decisión ni sujeta a su aplicación.

(6) El Supervisor Europeo de Protección de Datos, a quien se consultó de conformidad con el artículo 42, apartado 1, del Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo ([2]), emitió su dictamen el 24 de noviembre de 2022.

(7) Las medidas previstas en la presente Decisión se ajustan al dictamen del Comité establecido por el artículo 19, apartado 1, del Reglamento (UE) 2022/850.

([1]) (DO L 150 de 1.6.2022, p. 1).

([2]) Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, de 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) n.º 45/2001 y la Decisión n.º 1247/2002/CE (DO L 295 de 21.11.2018, p. 39).

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

Las normas y especificaciones técnicas mínimas, incluidas las relativas a la seguridad y los métodos de verificación de la integridad y la autenticidad, en las que se sustentan los componentes del sistema e-CODEX a que se refiere el artículo 5 del Reglamento (UE) 2022/850 serán las que figuran en el anexo de la presente Decisión.

Artículo 2

La presente Decisión entrará en vigor a los veinte días de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en Bruselas, el 20 de diciembre de 2022.

Por la Comisión
La Presidenta
Ursula VON DER LEYEN

ANEXO

Normas y especificaciones técnicas del sistema e-CODEX, incluidas las relativas a la seguridad y a los métodos de verificación de la integridad y la autenticidad

1. **INTRODUCCIÓN**

El presente anexo establece las normas y especificaciones técnicas mínimas, incluidas las relativas a la seguridad y a los métodos de verificación de la integridad y la autenticidad, de los componentes de e-CODEX.

2. **COMPONENTES DEL SISTEMA e-CODEX**

2.1. De conformidad con el artículo 5 del Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo ([1]), el sistema e-CODEX está integrado por:

a) un punto de acceso e-CODEX, compuesto por:

i) una pasarela;

ii) un conector;

b) unas especificaciones de procesamiento digital (DPS, por sus siglas en inglés);

c) los productos de soporte lógico (*software*), la documentación y otros recursos de apoyo enumerados en el anexo del Reglamento (UE) 2022/850:

i) el código fuente de la plataforma central de pruebas (CTP, por sus siglas en inglés);

ii) el código fuente de la herramienta de gestión de la configuración (CMT, por sus siglas en inglés);

iii) Metadata Workbench (MDW);

iv) el léxico de referencia de la UE para la justicia digital;

v) la documentación sobre la arquitectura.

2.2. Desde un punto de vista funcional, los elementos señalados se dividen en dos categorías: el kit de e-CODEX y los recursos implementables de e-CODEX.

2.3. **El kit de e-CODEX consta de lo siguiente:**

a) Documentación sobre la arquitectura de e-CODEX.

b) Código fuente del paquete del conector.

c) Código fuente de la herramienta de gestión de la configuración (CMT).

d) Código fuente de la plataforma central de pruebas (CTP).

e) Licencia de Metadata Workbench (MDW) de un tercero.

f) Léxico de referencia de la UE para la justicia digital.

g) Especificaciones de procesamiento digital (DPS).

a) Documentación sobre la arquitectura de e-CODEX

La documentación sobre la arquitectura consiste en un conjunto de documentos utilizados para proporcionar a las partes interesadas pertinentes conocimientos técnicos e informativos sobre la elección de las normas a las que deben ajustarse otros recursos del sistema e-CODEX. Dicha documentación define los requisitos y principios que se aplican a la hora de crear una comunicación transfronteriza interoperable para facilitar el intercambio electrónico de datos, lo que incluye cualquier contenido transmisible en formato electrónico. Además, en ella se enumeran las normas y las metodologías elegidas en las que se basa el sistema e-CODEX. La arquitectura garantiza la autonomía del sistema e-CODEX.

b) Código fuente del paquete del conector

El código fuente del paquete del conector se utiliza para crear los artefactos implementables que se describen en la sección 2.4.2.

([1]) Reglamento (UE) 2022/850 del Parlamento Europeo y del Consejo, de 30 de mayo de 2022, relativo a un sistema informatizado para el intercambio electrónico transfronterizo de datos en el ámbito de la cooperación judicial en materia civil y penal (sistema e-CODEX), y por el que se modifica el Reglamento (UE) 2018/1726 (DO L 150 de 1.6.2022, p. 1).

c) Herramienta de gestión de la configuración (CMT)

La herramienta de gestión de la configuración (CMT) es una herramienta web para gestionar los archivos de configuración asociados a la pasarela de eDelivery y al conector, y ofrece una forma estandarizada de ejecutar el proceso de configuración. La entidad que explota un punto de acceso e-CODEX autorizado puede acceder a la CMT a través de un portal disponible a escala mundial y cargar sus datos de configuración de eDelivery. Los datos cargados deben incluir la información de la configuración de red del nodo final de la pasarela, todos los certificados de seguridad necesarios para la conexión, así como los proyectos, los entornos y los casos de uso específicos en los que participe la entidad. La CMT debe comprobar automáticamente la validez de los datos cargados por la entidad que explota un punto de acceso e-CODEX autorizado y, en caso de que se produzcan errores, proporcionarle información de retorno.

Cuando se recibe la notificación de que se ha producido algún cambio en los datos facilitados por una entidad que explota un punto de acceso e-CODEX autorizado, debe generarse un nuevo paquete de configuración de e-CODEX (véase el punto 2.4.3) utilizando esta herramienta. Todas las entidades que explotan puntos de acceso e-CODEX autorizados deben ser notificadas de la creación del nuevo paquete de configuración de e-CODEX, que pueden descargar directamente de la CMT en cualquier momento. La CMT es capaz de proporcionar paquetes de configuración de e-CODEX para múltiples entornos informáticos, como PRUEBA, ACEPTACIÓN o PRODUCCIÓN.

Los nuevos paquetes de configuración de e-CODEX deben entrar en vigor siete días después de su creación, plazo en el que, si procede, las entidades que explotan puntos de acceso e-CODEX autorizados han de instalar el nuevo paquete en su entorno.

La CMT también mantiene a las entidades que explotan puntos de acceso e-CODEX autorizados al tanto de los tiempos de ejecución de sus certificados de seguridad y, cuando se aproxima la expiración de los certificados, lo notifica con antelación, por correo electrónico, a los puntos de acceso e-CODEX autorizados. En el caso de que una entidad que explota un punto de acceso e-CODEX autorizado deje expirar sus certificados de seguridad, estos deben retirarse automáticamente al crear el siguiente paquete.

La CMT debe alojarse de forma centralizada y estar disponible las veinticuatro horas del día, siete días a la semana, para los participantes en e-CODEX. La asistencia se limita al horario de oficina.

d) Plataforma central de pruebas (CTP)

La plataforma central de pruebas (CTP) de e-CODEX es una infraestructura de pruebas automatizada. Permite a las entidades que explotan puntos de acceso e-CODEX autorizados realizar pruebas de conectividad y pruebas de extremo a extremo entre sus infraestructuras e-CODEX y un punto de pruebas central fijo sin necesidad de que intervenga ningún otro socio (por ejemplo, otro punto de acceso e-CODEX autorizado) para probar las funcionalidades de comunicación. Además, permite enviar y recibir mensajes de prueba personalizables, lo que reduce el esfuerzo necesario para probar una infraestructura e-CODEX tanto en la fase de prueba inicial (instalación) como en la fase de pruebas por regresión. El progreso de los mensajes individuales, las pruebas establecidas por el Instituto Europeo de Normas de Telecomunicaciones (ETSI) para el correo electrónico certificado (REM) y los registros de errores son objeto de seguimiento y se presentan a las entidades que explotan puntos de acceso e-CODEX autorizados mediante procesos visuales específicamente concebidos.

La CTP consta de una pasarela e-CODEX, un conector, un conector-cliente y una interfaz gráfica de usuario web asociada [por ahora, interfaz de usuario (*frontend*)/servidor (*backend*) web basados en Nuxt.js] que pueden utilizarse para enviar mensajes a la pasarela de un socio, así como para visualizar mensajes enviados a la CTP por la misma pasarela. En la actualidad, la CTP almacena información operativa importante (variables locales) en una instancia de MongoDB y lee información de configuración (específica de una parte) procedente de la base de datos del conector. Además, utiliza la interfaz de programación de aplicaciones (API) de transferencia de estado representacional (REST) conector-cliente para recuperar información sobre los mensajes e-CODEX y enviar nuevos mensajes al conector y a la pasarela.

Con el fin de ofrecer una solución personalizable por cada entorno e-CODEX, la CTP se implementa en diversas instancias (copias) que existen en diversos entornos e-CODEX. Cada instancia de la CTP se implementa actualmente en un entorno UNIX (CentOS 7), en el que coexisten todos los componentes. Esto facilita la administración y el acceso al sistema de archivos, pero puede adaptarse para permitir una instalación en la que la infraestructura de mensajería e-CODEX se mantenga separada.

Cada usuario de la CTP está vinculado a una (1) pasarela. Para utilizar la CTP con fines de prueba, el único requisito es que la pasarela del punto de acceso e-CODEX autorizado exista en los modos-P del entorno específico de la CMT de e-CODEX.

e) Metadata Workbench

Metadata Workbench es una herramienta en la que se administra el léxico de referencia de la UE para la justicia digital. Permite a los modeladores semánticos mantener el léxico de manera sostenible adhiriéndose a la norma de modelización de la Especificación Técnica de Componente Básico, según se define en la documentación sobre la arquitectura de e-CODEX. Se trata de una solución de *software* como servicio (SaaS) en la web cuyo acceso está restringido exclusivamente a los administradores del léxico de referencia de la UE para la justicia digital. Metadata Workbench se desarrolla y explota en nombre del Ministerio de Justicia y Seguridad de los Países Bajos. Sobre la base de un acuerdo de licencia que debe celebrarse entre dicho Ministerio de Justicia y Seguridad y eu-LISA, esta obtendrá acceso a Metadata Workbench para administrar y explotar el léxico de referencia de la UE para la justicia digital.

f) Léxico de referencia de la UE para la justicia digital

El léxico de referencia de la UE para la justicia digital es un recurso para los términos y definiciones semánticos reutilizables empleado con el fin de garantizar la coherencia y la calidad de los datos a lo largo del tiempo y en todas las aplicaciones. Su repositorio semántico constituye la base de todas las estructuras de mensaje específicas de los casos de uso (esquemas XML).

La evolución futura del léxico de referencia para la justicia digital podría ajustarse a los vocabularios básicos ([2]). Para validar la conformidad con la especificación, podría crearse un validador basado en XML utilizando el servicio para la realización de pruebas de interoperabilidad ofrecido por la Comisión (Interoperability Test Bed).

g) Especificaciones de procesamiento digital (DPS)

Una especificación de procesamiento digital se refiere a las especificaciones técnicas para los modelos de proceso de negocio y los esquemas de datos que establecen la estructura electrónica de los datos intercambiados mediante el sistema e-CODEX basados en el léxico de referencia de la UE para la justicia digital. El modelo de proceso de negocio describe la ejecución técnica del procedimiento electrónico del instrumento jurídico respaldado por el sistema e-CODEX.

El modelo de proceso de negocio, unido al léxico de referencia de la UE para la justicia digital, da lugar a esquemas XML que describen la estructura electrónica de las DPS. Los esquemas XML permiten a los puntos de acceso autorizados enviar y recibir documentos con arreglo a lo dispuesto en un instrumento de cooperación judicial transfronteriza.

2.4. Los recursos implementables de e-CODEX

Los recursos implementables de e-CODEX son componentes del sistema que las entidades que explotan puntos de acceso autorizados implementan en sus entornos e-CODEX. eu-LISA se encargará de distribuirlos a dichas entidades (salvo en el caso de la pasarela).

Los recursos implementables son los siguientes:

a) Pasarela (punto 2.4.1).

b) Paquete del conector (punto 2.4.2).

c) Paquete de configuración de e-CODEX (incluidos los modos-P, los certificados públicos y los ajustes de seguridad) (punto 2.4.3).

d) Modelo de proceso o diseño de colaboración de negocio, como parte de las DPS.

e) Esquemas XML (estructuras de mensaje), como parte de las DPS.

2.4.1. *Pasarela*

Dentro del sistema e-CODEX, la pasarela es el módulo responsable del intercambio básico de comunicaciones. En la actualidad, una pasarela tiene implementadas las normas siguientes:

a) Norma ebMS 3.0 de OASIS ([3]): mensajes de intercambio entre pasarelas que se ajustan a la norma ebXML. Esta norma define la estructura que debe tener el encabezamiento de un mensaje para que sea comprensible en la infraestructura e-CODEX.

b) Perfil de mensajería de la Declaración de Aplicabilidad 4 (AS4) de OASIS: se trata de un perfil de conformidad de la especificación ebMS 3.0 de OASIS.

([2]) https://joinup.ec.europa.eu/collection/semantic-interoperability-community-semic/core-vocabularies

([3]) Organization for the Advancement of Structured Information Standards [Organización para la Mejora de las Normas de Información Estructurada].

c) Perfil Común del perfil AS4 de eDelivery ([4]).

Puede utilizarse cualquier solución de pasarela que cumpla los requisitos mencionados.

2.4.2. ***Paquete del conector***

El conector es un componente de enlace para conectar las aplicaciones nacionales específicas de DPS con las normas de mensajería genéricas de la pasarela. Así pues, este componente añade las características que se indican a continuación a la comunicación básica ya establecida por el componente de la pasarela:

a) **Pruebas ETSI-REM**: se trata de pruebas generadas por el conector en un formato XML firmado. La finalidad es informar al remitente sobre el tratamiento correcto o fallido de su mensaje. El conector genera y envía las pruebas en diferentes fases del tratamiento de un mensaje.

b) **Testigo TrustOK**: el conector remitente valida la integridad y la autenticación del documento objeto del mensaje (*business document*). El resultado de la validación se escribe en el testigo TrustOK, generado por un submódulo del conector: la biblioteca de seguridad.

c) **Contenedor ASiC-S**: de conformidad con la norma del ETSI EN 319 162-1 sobre firmas e infraestructuras electrónicas y contenedores de firmas asociadas (ASiC). El contenedor garantiza la autenticidad y la integridad de la carga útil transmitida por el conector.

d) **WS-Security**: a fin de incrementar la seguridad en la transmisión de los mensajes, el conector utiliza el protocolo WS-Security en el lado de la pasarela, así como en el lado del sistema conectado, para la transmisión. Por lo tanto, todo mensaje que el conector envía o recibe está cifrado y firmado.

e) **API común**: el conector ofrece una API estable que define los servicios web que se utilizan para la conexión a la pasarela y a la aplicación o las aplicaciones de los sistemas conectados. La estructura de los mensajes intercambiados con el conector también se describe en la API del conector.

Además del propio soporte lógico (*software*) del conector, el paquete también contiene un cliente de aplicación destinado a apoyar o sustituir un sistema conectado para el tratamiento de la mensajería e-CODEX.

Asimismo, se ha desarrollado un complemento especialmente para la pasarela Domibus ([5]) con el fin de conectar la API común del conector con el núcleo de procesamiento de la pasarela.

2.4.3. ***Paquete de configuración de e-CODEX***

En la comunicación basada en ebMS 3.0, un modo-P (o modo de procesamiento) regula la transmisión de todos los mensajes que intervienen en un intercambio de mensajes entre dos gestores de servicios de mensajería (MSH). Un paquete de configuración de e-CODEX comprende una colección de parámetros de configuración de mensajería (archivos de modo-P, varios almacenes de confianza de certificados, direcciones de red) que especifican detalladamente cómo tiene lugar la mensajería.

Los parámetros de configuración de la mensajería pueden clasificarse en las cinco categorías siguientes:

a) Parámetros relativos al remitente, tales como:

   i) identificador de la parte remitente;

   ii) certificado que utiliza el remitente para firmar sus mensajes;

   iii) autoridades de certificación en las que confía el remitente;

   iv) dirección (o direcciones) de red desde la que el remitente iniciará la comunicación.

b) Parámetros relativos al destinatario, tales como:

   i) identificador de la parte destinataria;

   ii) certificado que el destinatario espera que se utilice para cifrar los mensajes;

   iii) autoridades de certificación en las que confía el destinatario;

([4]) https://ec.europa.eu/digital-building-blocks/wikis/x/RqbXGw

([5]) La Comisión es responsable del mantenimiento de la pasarela Domibus (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) dirección (o direcciones) de red desde la que el destinatario aceptará la comunicación entrante.

c) Parámetros relativos al par remitente-destinatario, tales como (en caso de usarse):

i) identificador de acuerdo, identificador de modo-P.

d) Parámetros relativos a las DPS, tales como:

i) función (o funciones) de la parte remitente;

ii) función (o funciones) de la parte destinataria;

iii) servicio (o servicios);

iv) acción (o acciones) dentro del servicio.

e) Parámetros relacionados con el uso del protocolo de mensajería, o el perfil del protocolo de mensajería.

En e-CODEX, todos los archivos de configuración relativos a un MSH o un dominio se agrupan en un archivo principal que puede utilizarse para la configuración de la pasarela y del conector.

El archivo principal define una red de comunicación individual a la que el MSH puede dirigirse durante su funcionamiento. Es necesario que la configuración se genere de forma centralizada, ya que toda la información de todos los puntos de acceso e-CODEX autorizados debe estar disponible para la generación del paquete de configuración de e-CODEX, que es creado por la CMT.

3. SEGURIDAD Y MÉTODOS PARA LA VERIFICACIÓN DE LA INTEGRIDAD Y LA AUTENTICIDAD DEL SISTEMA e-CODEX

e-CODEX es un sistema de comunicación que ofrece una base sólida para dar respuesta a los requisitos de seguridad y protección de datos. En particular, el sistema e-CODEX presenta las características técnicas necesarias para cumplir todos los requisitos establecidos en el Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo ([6]).

3.1. Seguridad desde el diseño:

El sistema e-CODEX es, desde un punto de vista técnico, un mecanismo de transporte. Existen distintas capas pertinentes para la seguridad:

a) una capa de red;

b) una capa de transporte;

c) una capa de mensaje;

d) una capa de documento.

En cada una de estas capas se aplican medidas de seguridad.

3.1.1. *Capa de red*

e-CODEX puede utilizarse con distintos tipos de capas de red. La capa de red suele aplicarse a las conexiones normales a internet. Por lo tanto, la seguridad se basa en las aplicaciones de seguridad habituales de la tecnología de internet (ampliada por las otras capas descritas en el presente punto). En la mayoría de los casos de uso de e-CODEX, tal capa de red es suficiente. Para unos requisitos de seguridad más estrictos, podría aplicarse una capa de red adicional. Asimismo, pueden tenerse en cuenta otras redes.

3.1.2. *Capa de transporte*

La capa de transporte suele estar protegida por el protocolo TLS (seguridad de la capa de transporte) o mTLS (TLS mutua). Se trata de una norma consolidada para proteger la capa de transporte en las tecnologías de internet, aplicada en todo el mundo a un gran número de servicios. Los protocolos TLS o mTLS proporcionan el cifrado y la autenticación en el canal de transporte. Garantizan la seguridad de la ruta de transporte entre sus distintos concentradores. Cada concentrador debe descifrar (solo) los datos de dirección para reenviar el mensaje al siguiente concentrador. Antes del reenvío, el concentrador cifra de nuevo los datos de dirección. Si bien existe un protocolo SLT simple (unidireccional), y a veces se sigue aplicando, se recomienda aplicar el protocolo SLT bidireccional (mTLS), ya que se está convirtiendo en la norma actual para la protección de la capa de transporte.

([6]) Reglamento (UE) n.º 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE (DO L 257 de 28.8.2014, p. 73).

3.1.3. ***Capa de mensaje***

En la capa de mensaje, hay distintos componentes de e-CODEX que aplican varias normas:

a) El protocolo utilizado para la transmisión de pasarela a pasarela (como capa de mensaje) es AS4, que firma y cifra los mensajes (dependiendo de la configuración de seguridad a nivel de pasarela).

b) El componente básico del sistema e-CODEX es el conector. Añade seguridad a la capa de mensaje mediante el uso del protocolo WS-Security a efectos de la firma y el cifrado de mensajes para los servicios web hacia la pasarela y el servidor (o los servidores) (*backend*). Por lo tanto, se aplica un cifrado de conector a conector de manera adicional.

c) Para la funcionalidad de firma y cifrado en los sistemas e-CODEX se utilizan certificados digitales. Estos certificados digitales de cifrado y firma se ajustan a la norma X.509.

3.1.4. ***Capa de documento***

Los mensajes contienen documentos y ficheros adjuntos, que se agrupan en un paquete denominado «contenedor». El contenedor se construye de acuerdo con la norma ASiC-S. El conector remitente firma el contenedor ASiC-S, y la firma se valida en el momento de la recepción por el conector destinatario.

3.2. **Métodos de verificación de la integridad y la autenticidad**

3.2.1. ***Acceso a la configuración e-CODEX***

La comunicación entre los puntos de acceso e-CODEX requiere una configuración previa. Esta configuración se realiza a través del paquete de configuración de e-CODEX, que contiene los datos de direccionamiento, la política de seguridad aplicada y otra información. Además, contiene los almacenes de confianza con los certificados públicos de todos los puntos de acceso e-CODEX participantes. Un «coordinador para la configuración» (CfC) central crea los archivos para la configuración de cada socio, empleando la herramienta de gestión de la configuración (CMT). El acceso a esta CMT se concede de manera exclusiva a cada socio, previa petición personal e individual. El acceso administrativo, gestionado por eu-LISA, está restringido a los CfC.

3.2.2. ***Firmas y sellos electrónicos admitidos***

El sistema e-CODEX debe admitir todos los tipos de sellos electrónicos y firmas electrónicas, tal como se establece en el Reglamento (UE) n.º 910/2014.

3.2.3. ***Testigo TrustOK de e-CODEX***

El conector remitente valida la firma de las DPS de un mensaje. El resultado de la validación se escribe en el testigo TrustOK de e-CODEX, generado por una biblioteca de seguridad, que es un submódulo del conector. La validación de la firma electrónica la realiza el conector e-CODEX utilizando herramientas de DSS (servicios de firma digital).

3.2.4. ***Testigo legible electrónicamente (XML)***

El testigo legible electrónicamente se presenta como un archivo XML subyacente a un determinado esquema que contiene toda la información sobre la firma del testigo del mensaje (*business token*) y el informe de validación resultante de la validación jurídica y técnica.

3.2.5. ***Testigo legible por el ser humano (PDF)***

El PDF consta de tres partes. La primera parte, presentada en la primera página del propio testigo, contiene información general sobre el sistema electrónico avanzado y una evaluación de la validez jurídica del documento objeto del mensaje (*business document*). Además, en la parte inferior de la página figuran una cláusula de exención de responsabilidad y un «sello de validación» con el resultado de la validación jurídica (correcta/fallida).

Un sistema electrónico avanzado es un sistema conectado capaz de identificar de forma segura al usuario y garantizar la integridad de los mensajes enviados a través del sistema entre el cliente y el conector e-CODEX.

La segunda parte, en la segunda página, ofrece una visión técnica general estandarizada de la información del informe de validación original. La información del resumen técnico variará en función del sistema conectado (basado en autenticación o en firma). Un testigo basado en la firma contendrá la información facilitada por el certificado subyacente, incluidos los atributos (si están disponibles). Un testigo basado en la autenticación contendrá el nombre de la institución desde la que se haya enviado el documento y, cuando se facilite, el nombre del autor del documento.

En la parte inferior de la página figuran un sello del color del resultado de la validación técnica de los documentos (verde/amarillo/rojo) y una breve descripción, por ejemplo, con información adicional sobre el motivo por el que un documento ha recibido una evaluación técnica amarilla.

La tercera parte del documento consiste en el informe de validación original creado por el programa informático de validación del Estado miembro emisor.

4. ESPECIFICACIONES DE PROCESAMIENTO DIGITAL (DPS) DESARROLLADAS HASTA LA FECHA

Servicio de justicia electrónica	DPS: modelo de proceso	DPS: esquema XML	Origen del proyecto
Requerimiento europeo de pago	√	√	e-CODEX
Demandas de escasa cuantía	√	√	e-CODEX
Orden de detención europea	√	√	e-CODEX
Sanciones económicas	√	√	e-CODEX
Cooperación judicial	√	√	e-CODEX
Decisión Marco 909 (penas privativas de libertad)	√	√	e-CODEX
Asuntos matrimoniales	√	√	e-SENS
Orden europea de retención de cuentas	√	√	e-SENS
Registro de Actos de Última Voluntad	√	√	e-SENS
Notificación de documentos	√	√	e-CODEX