DECISÃO DE EXECUÇÃO (UE) 2022/2519 DA COMISSÃO

de 20 de dezembro de 2022

relativa às normas e especificações técnicas para o sistema e-CODEX, incluindo de segurança e aos métodos de verificação da integridade e da autenticidade

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo a um sistema informatizado de intercâmbio eletrónico transfronteiriço de dados no domínio da cooperação judiciária em matéria civil e penal (sistema e-CODEX) e que altera o Regulamento (UE) 2018/1726 ([1]), nomeadamente o artigo 6.º, n.º 1, alínea a),

Considerando o seguinte:

(1) Em conformidade com o artigo 5.º do Regulamento (UE) 2022/850, o sistema e-CODEX é composto por um ponto de acesso e-CODEX, normas processuais digitais e os produtos de *software*, a documentação e outros recursos de apoio enumerados no anexo do referido regulamento.

(2) O ponto de acesso e-CODEX é composto por uma porta de ligação, que consiste num *software*, que tem por base um conjunto comum de protocolos, e que permite o intercâmbio seguro de informações numa rede de telecomunicações com outras portas de ligação que utilizam o mesmo conjunto comum de protocolos, e de um conector, que permite estabelecer a conexão entre sistemas ligados à porta de ligação, e que consiste num *software*, que tem por base um conjunto comum de protocolos abertos.

(3) Tendo em vista o êxito do processo de transferência e tomada de controlo do sistema e-CODEX para a eu-LISA, e a fim de permitir o cumprimento das atribuições pelas quais a eu-LISA será responsável, deverão ser estabelecidas as normas e especificações técnicas mínimas, incluindo de segurança e os métodos de verificação da integridade e da autenticidade, subjacentes aos componentes do sistema e-CODEX.

(4) Nos termos dos artigos 1.º e 2.° do Protocolo n.º 22 relativo à posição da Dinamarca, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, a Dinamarca não participou na adoção do Regulamento (UE) 2022/850, não estando, por conseguinte, vinculada nem sujeita à aplicação da presente decisão.

(5) Nos termos dos artigos 1.º e 2.° e do artigo 4.º-A, n.º 1, do Protocolo n.º 21 relativo à posição do Reino Unido e da Irlanda em relação ao espaço de liberdade, segurança e justiça, anexo ao Tratado da União Europeia e ao Tratado sobre o Funcionamento da União Europeia, e sem prejuízo do artigo 4.º do referido protocolo, a Irlanda não participou na adoção do Regulamento (UE) 2022/850, não estando, por conseguinte, vinculada nem sujeita à aplicação da presente decisão.

(6) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([2]) e emitiu um parecer em 24 de novembro de 2022.

(7) As medidas previstas na presente decisão estão em conformidade com o parecer do comité estabelecido pelo artigo 19.º, n.º 1, do Regulamento (UE) 2022/850,

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

([2]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

ADOTOU A PRESENTE DECISÃO:

Artigo 1.º

As normas e especificações técnicas mínimas, incluindo de segurança e os métodos de verificação da integridade e da autenticidade, subjacentes aos componentes do sistema e-CODEX a que se refere o artigo 5.º do Regulamento (UE) 2022/850 são os estabelecidos no anexo da presente decisão.

Artigo 2.º

A presente decisão entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

Feito em Bruxelas, em 20 de dezembro de 2022.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

Normas e especificações técnicas para o sistema e-CODEX, incluindo de segurança e os métodos de verificação da integridade e da autenticidade

1. **INTRODUÇÃO**

O presente anexo estabelece as normas e especificações técnicas mínimas para o sistema e-CODEX, incluindo de segurança e os métodos de verificação da integridade e da autenticidade.

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

2.1. Nos termos do artigo 5.º do Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho ([1]), o sistema e-CODEX é composto por:

a) Um ponto de acesso e-CODEX, que consiste em:

i) uma porta de ligação;

ii) um conector;

b) Normas processuais digitais (DPS);

c) Os produtos de *software*, a documentação e outros recursos de apoio enumerados no anexo do Regulamento (UE) 2022/850:

i) o código-fonte da Plataforma Central para Realização de Ensaios (CTP),

ii) o código-fonte da Ferramenta de Gestão da Configuração (CMT),

iii) a ferramenta *Metadata Workbench* (MDW),

iv) o Vocabulário de Base da Justiça Eletrónica da UE,

v) a documentação da arquitetura.

2.2. De um ponto de vista funcional, estes elementos dividem-se em duas categorias: o conjunto de instrumentos do e-CODEX e os recursos implantáveis do e-CODEX.

2.3. **O conjunto de instrumentos do e-CODEX é composto pelo/a(s):**

a) Documentação da arquitetura do e-CODEX;

b) Código-fonte do conjunto de conectores;

c) Código-fonte da Ferramenta de Gestão da Configuração (CMT);

d) Código-fonte da Plataforma Central para Realização de Ensaios (CTP);

e) Licença da ferramenta *Metadata Workbench* (MDW) emitida por um terceiro;

f) Vocabulário de Base da Justiça Eletrónica da UE;

g) Normas processuais digitais (DPS).

a) Documentação da arquitetura do e-CODEX

A documentação da arquitetura consiste num conjunto de documentos utilizados para facultar conhecimentos técnicos e informativos às partes interessadas pertinentes sobre a escolha das normas a que devem obedecer outros recursos do sistema e-CODEX. Estes documentos definem os requisitos e princípios aplicáveis à criação de comunicações transfronteiriças interoperáveis para facilitar o intercâmbio eletrónico de dados, o que inclui qualquer conteúdo transmissível em formato eletrónico. Além disso, enumera as normas e metodologias escolhidas em que se baseia o sistema e-CODEX. A arquitetura assegura a autonomia do sistema e-CODEX.

b) Código-fonte do conjunto de conectores

O código-fonte do conjunto de conectores é utilizado para criar os artefactos implantáveis descritos no capítulo 2.4.2.

([1]) Regulamento (UE) 2022/850 do Parlamento Europeu e do Conselho, de 30 de maio de 2022, relativo a um sistema informatizado de intercâmbio eletrónico transfronteiriço de dados no domínio da cooperação judiciária em matéria civil e penal (sistema e-CODEX) e que altera o Regulamento (UE) 2018/1726 (JO L 150 de 1.6.2022, p. 1).

c) Ferramenta de Gestão da Configuração (CMT)

A Ferramenta de Gestão da Configuração (CMT) é uma ferramenta em linha para gestão dos ficheiros de configuração associados à porta de ligação *e-Delivery* e ao conector, proporcionando uma forma normalizada de gerir o fluxo de trabalho de configuração. A entidade que opera um ponto de acesso e-CODEX autorizado pode aceder à CMT através de um portal disponível a partir de qualquer ponto do mundo e carregar os seus dados de configuração *e-Delivery*. Os dados carregados devem incluir as informações de configuração da rede terminal da porta de ligação, todos os certificados de segurança necessários para a ligação, bem como os projetos, ambientes e casos de utilização específicos conexos. A CMT deve verificar automaticamente a validade dos dados carregados e, caso ocorram erros, reportar a informação à entidade que opera os pontos de acesso e-CODEX autorizados.

Sempre que é recebida uma notificação relativa a alterações dos dados fornecidos por uma entidade que opera um ponto de acesso e-CODEX autorizado, um novo pacote de configuração do e-CODEX (ver ponto 2.4.3) deve ser concebido utilizando esta ferramenta. Todas as entidades que operam os pontos de acesso do e-CODEX autorizados devem ser notificadas da criação do novo pacote de configuração e-CODEX e podem descarregá-lo diretamente da CMT, a qualquer momento. A CMT pode fornecer pacotes de configuração e-CODEX para múltiplos ambientes informáticos, tais como os ambientes de teste, de aceitação ou de produção.

Os novos pacotes de configuração e-CODEX devem entrar em funcionamento sete dias após a sua criação e, se aplicável, as entidades que operam os pontos de acesso e-CODEX autorizados devem instalar o novo pacote no seu ambiente até essa data.

A CMT também mantém informada a entidade que opera os pontos de acesso e-CODEX autorizados relativamente aos períodos de execução dos seus certificados de segurança e notifica antecipadamente os pontos de acesso e-CODEX autorizados, por correio eletrónico, sobre a expiração futura do seu certificado. Se uma entidade que opera um ponto de acesso e-CODEX autorizado deixar expirar os seus certificados de segurança, estes devem ser automaticamente retirados da criação do pacote seguinte.

A CMT deverá ser alojada a nível central e estar disponível para os intervenientes do e-CODEX 24 horas por dia, sete dias por semana. A prestação de apoio só pode ser realizada durante as horas de expediente.

d) Plataforma Central para Realização de Ensaios (CTP)

A Plataforma Central para Realização de Ensaios do e-CODEX (CTP) é uma infraestrutura de testes automatizada. Esta plataforma permite que a entidade que opera um ponto de acesso e-CODEX autorizado realize testes de conectividade e testes de extremo-a-extremo entre a sua infraestrutura e-CODEX e um ponto de testes central definido, sem necessidade de envolver qualquer outro parceiro (p. ex., outro ponto de acesso e-CODEX autorizado) a fim de testar as funcionalidades de comunicação. A CTP permite enviar e receber mensagens de teste personalizáveis, reduzindo assim o esforço necessário para testar uma infraestrutura e-CODEX, tanto no momento inicial (instalação) como durante os testes de regressão. O estado das mensagens individuais, as provas de correio eletrónico registado (REM) do Instituto Europeu de Normalização das Telecomunicações (ETSI) e os registos de erros são acompanhados e apresentados às entidades que operam os pontos de acesso e-CODEX autorizados através de processos visuais especificamente concebidos.

A CTP é composta por uma porta de ligação e-CODEX, um conector, um conector-cliente e uma interface gráfica de utilizador em linha associada [a interface frontal e a infraestrutura de base (*frontend*/*backend*) em linha atuais foram concebidas em Nuxt.js], que pode ser utilizada para enviar mensagens para uma porta de ligação de um parceiro, bem como para visualizar mensagens enviadas ao CTP a partir da mesma porta de ligação. A CTP armazena atualmente importantes informações operacionais (variáveis locais) numa instância MongoDB e lê informações de configuração (de uma parte) da base de dados do conector. Além disso, utiliza a interface de programação de aplicações (API) com transferência de estado representacional (REST) do conector-cliente a fim de obter informações sobre as mensagens e-CODEX e enviar novas mensagens para o conector e a porta de ligação.

A fim de proporcionar uma solução personalizável para cada ambiente e-CODEX, a CTP é implantada em várias instâncias (cópias) que existem em vários ambientes e-CODEX. Cada instância da CTP está atualmente implantada num ambiente UNIX (CentOS 7), onde coexistem todos os componentes. Esta configuração facilita a administração e o acesso ao sistema de ficheiros, mas pode ser adaptada a fim de ter em conta as instalações em que a infraestrutura de mensagens e-CODEX é mantida à parte.

Cada utilizador da CTP está ligado a uma (1) porta de ligação. O único requisito para utilizar a CTP para testes é que a porta de ligação desse ponto de acesso e-CODEX autorizado exista nos *P-Modes* (modos de processamento) para esse ambiente específico e-CODEX da CMT.

e) A *Metadata Workbench*

A *Metadata Workbench* é uma ferramenta onde é administrado o Vocabulário de Base da Justiça Eletrónica da UE. Esta ferramenta permite que os modeladores de dados semânticos mantenham o vocabulário de forma sustentável, respeitando a norma de modelização das Especificações Técnicas dos Componentes Fundamentais, tal como definida na documentação da arquitetura e-CODEX. Trata-se de uma solução do tipo *software* como serviço (SaaS) em linha, com acesso limitado apenas aos administradores do Vocabulário de Base da Justiça Eletrónica da UE. A *Metadata Workbench* é desenvolvida e gerida em nome do Ministério da Justiça e da Segurança dos Países Baixos. Com base num acordo de licença a celebrar entre o Ministério da Justiça e da Segurança e a eu-LISA, a eu-LISA terá acesso à *Metadata Workbench* a fim de administrar e gerir o Vocabulário de Base da Justiça Eletrónica da UE.

f) Vocabulário de Base da Justiça Eletrónica da UE

O Vocabulário de Base da Justiça Eletrónica da UE é um recurso para termos semânticos e definições reutilizáveis usado para garantir a coerência e qualidade dos dados ao longo do tempo e em todos os casos de utilização. No seu repositório semântico, estão armazenadas todas as estruturas de mensagens específicas aos casos de utilização (esquemas XML).

As evoluções futuras do Vocabulário de Base da Justiça Eletrónica poderão ser realizadas em conformidade com os Vocabulários de Base ([2]). A fim de validar a conformidade com a especificação, pode ser criado um validador baseado em XML utilizando o serviço do Banco de Testes de Interoperabilidade disponibilizado pela Comissão.

g) Normas processuais digitais (DPS)

Uma norma processual digital consiste nas especificações técnicas para os modelos dos processos operacionais e esquemas de dados que determinam a estrutura eletrónica dos dados trocados através do sistema e-CODEX com base no Vocabulário de Base da Justiça Eletrónica da UE. O modelo do processo operacional descreve a aplicação técnica do procedimento eletrónico do instrumento jurídico que é compatível com o sistema e-CODEX.

O modelo do processo operacional, juntamente com o Vocabulário de Base da Justiça Eletrónica da UE, resulta em esquemas XML que descrevem a estrutura eletrónica das DPS. Os esquemas XML permitem que os pontos de acesso autorizados enviem e recebam documentos, tal como previsto num instrumento de cooperação judiciária transfronteiriço.

2.4. **Recursos implantáveis do e-CODEX**

Os recursos implantáveis do e-CODEX são componentes do e-CODEX implantados por entidades que operam um ponto de acesso e-CODEX autorizado no seu ambiente e-CODEX. Com exceção da porta de ligação, estes recursos devem ser distribuídos pela eu-LISA às entidades que operam um ponto de acesso e-CODEX autorizado.

Os recursos implantáveis são:

a) A porta de ligação (ponto 2.4.1);

b) O conjunto de conectores (ponto 2.4.2);

c) O pacote de configuração e-CODEX (incluindo os *P-Modes*, os certificados e configurações de segurança públicos) (ponto 2.4.3);

d) O plano de colaboração ou o modelo do processo operacional no âmbito das DPS;

e) Os esquemas XML são estruturas de mensagem integradas nas DPS.

2.4.1. ***A porta de ligação***

A porta de ligação é o módulo responsável pelo intercâmbio básico de comunicações no sistema e-CODEX. Atualmente, uma porta de ligação aplica as seguintes normas:

a) Norma OASIS ([3]) ebMS 3.0: mensagens de intercâmbio das portas de ligação conformes com a norma ebXML. Esta norma define a estrutura que o cabeçalho da mensagem deve ter a fim de ser compreendido no âmbito das infraestruturas e-CODEX;

b) Perfil de mensagens da Declaração de Aplicabilidade OASIS 4 (AS4): trata-se de um perfil de conformidade da especificação OASIS ebMS 3.0;

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

([3]) Organização para o Avanço de Normas de Informação Estruturadas (*Organization for the Advancement of Structured Information Standards*).

c) O perfil AS4 do Perfil Comum do *eDelivery* ([4]).

Pode ser utilizada qualquer solução de porta de ligação que cumpra esses requisitos.

2.4.2. ***Conjunto de conectores***

O conector é um componente de ligação que serve para ligar aplicações nacionais específicas das DPS às normas de transmissão de mensagens genéricas da porta de ligação. Desta forma, este componente acrescenta as seguintes funcionalidades à comunicação de base já estabelecida pelo componente «porta de ligação»:

a) **Provas ETSI-REM**: provas geradas pelo conector num formato XML assinado. O objetivo dessas provas é informar o remetente de uma mensagem sobre o tratamento bem ou mal sucedido da mensagem. As provas são geradas e enviadas pelo conector em diferentes fases do processamento de mensagens;

b) Mecanismo de autenticação **TrustOK Token**: O conector remetente valida a integridade e a autenticação do documento operacional na mensagem. O resultado desta validação é inscrito no *TrustOK Token*. Este mecanismo de autenticação (*token*) é gerado por um submódulo do conector, a biblioteca de segurança;

c) **Contentor ASiC-S**: Em conformidade com a norma EN 319 162-1 do ETSI em matéria de Assinaturas e Infraestruturas Eletrónicas e Contentores de Assinaturas Associadas (ASiC). O contentor garante a autenticidade e a integridade dos dados da carga útil transmitida pelo conector;

d) ***WS-Security* (mecanismo de segurança dos serviços Web)**: Para aumentar a segurança da transmissão das mensagens, o conector utiliza a *WS-Security* do lado da porta de ligação, bem como do lado do sistema conectado para a transmissão. Esta utilização da *WS-Security* significa que todas as mensagens que o conector envia ou recebe são encriptadas e assinadas;

e) **API comum**: O conector disponibiliza uma API estável que define os serviços Web que são utilizados na ligação entre a porta de ligação e a(s) aplicação(ões) dos sistemas conectados. A estrutura das mensagens trocadas com o conector é também descrita na API do Conector.

Para além do próprio *software* conector, o conjunto contém também uma aplicação-cliente destinada a apoiar ou substituir um sistema conectado para o tratamento de mensagens e-CODEX.

Além disso, foi desenvolvida uma extensão com a finalidade específica de permitir à porta de ligação Domibus ([5]) ligar a API comum do conector ao núcleo de processamento da porta de ligação.

2.4.3. ***Pacote de configuração do e-CODEX***

Na comunicação baseada na ebMS 3.0, um modo *P-Mode* (ou modo de processamento) rege a transmissão de todas as mensagens envolvidas num intercâmbio de mensagens entre dois Gestores do Serviço de Troca de Mensagens (MSH). Um pacote de configuração do e-CODEX inclui um conjunto de parâmetros de configuração da troca de mensagens [ficheiros *P-Mode*, vários repositórios de confiança (*trust stores*) de certificados, endereços de rede] que especificam em pormenor a forma como se efetua a troca de mensagens.

Os parâmetros de configuração da troca de mensagens podem ser classificados nas cinco categorias seguintes:

a) Parâmetros relativos ao remetente, tais como:

   i) o identificador do remetente,

   ii) o certificado utilizado pelo remetente para assinar as mensagens,

   iii) as autoridades de certificação de confiança do remetente,

   iv) o endereço (ou endereços) da rede a partir do qual o remetente inicia a comunicação;

b) Parâmetros relativos ao destinatário, tais como:

   i) o identificador do destinatário,

   ii) o certificado que o destinatário espera que seja utilizado para encriptar as mensagens,

   iii) as autoridades de certificação de confiança do destinatário,

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

([5]) A porta de ligação Domibus é mantida pela Comissão (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus)

iv) o endereço (ou endereços) da rede a partir do qual o destinatário aceita a comunicação recebida;

c) Parâmetros relativos ao par remetente-destinatário (se utilizados), tais como:

i) o identificador do acordo, o identificador do *P-Mode*;

d) Parâmetros relativos às DPS, tais como:

i) a(s) função(ões) do remetente,

ii) a(s) função(ões) do destinatário,

iii) o(s) serviço(s),

iv) as ações no âmbito do serviço.

e) Parâmetros relativos à utilização do protocolo de troca de mensagens ou o perfil do protocolo de troca de mensagens.

No e-CODEX, todos os ficheiros de configuração relativos a um MSH ou a um domínio são agrupados num ficheiro principal que pode ser utilizado para a configuração da porta de ligação e do conector.

O ficheiro principal define uma rede de comunicação individual que o MSH pode utilizar durante o seu funcionamento. É necessário que a configuração seja gerada centralmente, uma vez que todas as informações de todos os pontos de acesso e-CODEX autorizados têm de estar disponíveis para a geração do pacote de configuração e-CODEX, que é criado pela CMT.

3. SEGURANÇA E MÉTODOS DE VERIFICAÇÃO DA INTEGRIDADE E DA AUTENTICIDADE DO SISTEMA E-CODEX

O sistema e-CODEX é um sistema de comunicação que presta um importante apoio no cumprimento dos requisitos em matéria de segurança e de proteção de dados. Em especial, o sistema e-CODEX proporciona as funcionalidades técnicas necessárias ao cumprimento de todos os requisitos previstos no Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho ([6]).

3.1. Segurança desde a fase de conceptualização

O sistema e-CODEX é, do ponto de vista técnico, um mecanismo de transporte. Existem diferentes camadas relevantes para a segurança:

a) Uma camada de rede;

b) Uma camada de transporte;

c) Uma camada de mensagens;

d) Uma camada de documento.

Em cada uma destas camadas são aplicadas medidas de segurança.

3.1.1. *Camada de rede*

O e-CODEX pode ser utilizado com diferentes tipos de camadas da rede. É geralmente aplicado em ligações normais à Internet. Por conseguinte, a segurança segue as aplicações de segurança habituais em matéria de tecnologias da Internet (e é ampliada pelas outras camadas descritas no presente ponto). Para a maioria dos casos de utilização do e-CODEX, essa camada de rede é suficiente. Em caso de requisitos de segurança mais elevados, poderia também ser aplicada uma camada de rede adicional. Pode igualmente considerar-se a utilização de outras redes.

3.1.2. *Camada de transporte*

A camada de transporte é geralmente protegida pela Segurança da Camada de Transporte (TLS) ou pela mTLS (TLS mútua). Trata-se de uma norma bem estabelecida para proteger a camada de transporte nas tecnologias da Internet e é aplicada a nível mundial num grande número de serviços. A TLS/mTLS encarrega-se da encriptação e da autenticação no canal de transporte. Garante a segurança do itinerário de transporte entre cada plataforma de transporte. Cada plataforma tem de desencriptar (apenas) os dados do endereço a fim de enviar a mensagem para a plataforma seguinte. Antes do envio, cada plataforma encripta novamente os dados do endereço. É possível utilizar uma TLS simples (unidirecional) que, por vezes, ainda é aplicada, mas recomenda-se a utilização de uma TLS bidirecional (mTLS), uma vez que se está a tornar a norma estabelecida para a proteção da camada de transporte.

([6]) Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à identificação eletrónica e aos serviços de confiança para as transações eletrónicas no mercado interno e que revoga a Diretiva 1999/93/CE (JO L 257 de 28.8.2014, p. 73).

3.1.3. ***Camada de mensagens***

Na camada de mensagens, são aplicadas várias normas por diferentes componentes do e-CODEX:

a) O protocolo AS4 é utilizado para a transmissão porta de ligação-a-porta de ligação (como camada de mensagens), assinando e encriptando as mensagens consoante a configuração de segurança ao nível da porta de ligação;

b) O componente fundamental do sistema e-CODEX é o conector. Este componente aumenta a segurança da camada de mensagens, utilizando a *WS-Security* para assinar e encriptar as mensagens para os serviços Web encaminhadas para a porta de ligação e para a infraestrutura de base (*backend*). Por conseguinte, é aplicada uma encriptação conector-a-conector adicional;

c) São utilizados certificados digitais para a funcionalidade de assinatura e encriptação em todos os sistemas e-CODEX. Esses certificados digitais de encriptação e assinatura estão em conformidade com a norma X.509.

3.1.4. ***Camada de documento***

As mensagens contêm documentos e anexos. Estes são compilados num pacote denominado «contentor». O contentor é concebido de acordo com a norma ASiC-S. O conector remetente assina o contentor ASiC-S e a assinatura é validada pelo conector destinatário no momento da receção.

3.2. **Métodos de verificação da integridade e da autenticidade**

3.2.1. ***Acesso à configuração do e-CODEX***

A comunicação entre os pontos de acesso e-CODEX necessita de uma configuração prévia. Esta configuração é feita através do pacote de configuração do e-CODEX. O pacote de configuração contém os dados relativos ao endereçamento, a política de segurança aplicada e outras informações. Além disso, contém também os repositórios de confiança (*trust stores*) com os certificados públicos de todos os pontos de acesso e-CODEX intervenientes. Os ficheiros de configuração são criados para a configuração de cada parceiro por um «Coordenador de Configuração» central (CFC) utilizando a Ferramenta de Gestão da Configuração (CMT). O acesso a esta CMT é limitado, sendo facultado a cada parceiro apenas mediante um pedido pessoal e individual. O acesso administrativo é limitado aos CFC, que são geridos pela eu-LISA.

3.2.2. ***Assinaturas e selos eletrónicos suportados***

O sistema e-CODEX deve suportar todos os tipos de selos eletrónicos e assinaturas eletrónicas, tal como previsto no Regulamento (UE) n.º 910/2014.

3.2.3. ***TrustOK Token do e-CODEX***

O conector remetente valida a assinatura do DPS de uma mensagem. O resultado desta validação é inscrito no *TrustOK Token* do e-CODEX. Este mecanismo de autenticação (*token*) é gerado por um submódulo do conector, a biblioteca de segurança. A validação da assinatura eletrónica é efetuada pelo conector e-CODEX utilizando ferramentas DSS (serviço de assinaturas digitais).

3.2.4. ***Mecanismo de autenticação (token) legível por máquina (XML)***

O mecanismo de autenticação (*token*) legível por máquina consiste num ficheiro XML subjacente a um determinado esquema que contém todas as informações sobre a assinatura do mecanismo de autenticação (*token*) operacional e o relatório de validação resultante da validação jurídica e técnica.

3.2.5. ***Mecanismo de autenticação (token) para leitura humana (PDF)***

O ficheiro PDF é composto por três partes. A primeira parte, apresentada na primeira página do próprio mecanismo de autentificação (*token*), inclui informações gerais sobre o sistema eletrónico avançado e uma avaliação da validade jurídica do documento operacional. Além disso, no final da página está presente uma declaração de exoneração de responsabilidade e um «carimbo de validação» com o resultado da validação legal (aprovada/não aprovada).

Um sistema eletrónico avançado é um sistema conectado capaz de identificar de forma segura o utilizador e de garantir a integridade das mensagens enviadas entre o cliente e o conector e-CODEX através desse sistema.

A segunda parte, na segunda página, apresenta uma panorâmica técnica normalizada das informações constantes do relatório de validação original. As informações constantes da panorâmica técnica variam consoante o sistema conectado (baseado em autenticações ou assinaturas). Um mecanismo de autenticação (*token*) baseado em assinaturas contém as informações constantes do certificado subjacente, incluindo os atributos (se disponíveis). Um mecanismo de autenticação (*token*) baseado em autenticações contém o nome da instituição a partir da qual o documento foi enviado e, quando fornecido, o nome do autor do documento.

No final desta página está presente um carimbo de cor correspondente ao resultado da validação técnica dos documentos (verde/amarelo/vermelho) e uma breve descrição, por exemplo, fornecendo informações adicionais sobre as razões que justificam que o documento tenha recebido uma avaliação técnica amarela.

A terceira parte do documento consiste no relatório de validação original, tal como foi criado pelo *software* de validação do Estado-Membro emissor.

4. NORMAS PROCESSUAIS DIGITAIS (DPS) CONCEBIDAS ATÉ À PRESENTE DATA

Serviço e-Justice	DPS: modelo do processo	DPS: Esquema XML	Fonte do projeto
Injunção de pagamento europeia	√	√	e-CODEX
Ações de pequenos montantes	√	√	e-CODEX
Mandado de detenção europeu	√	√	e-CODEX
Sanções Pecuniárias	√	√	e-CODEX
AJM	√	√	e-CODEX
DQ 909 (Penas privativas de liberdade)	√	√	e-CODEX
Matéria matrimonial	√	√	e-SENS
Decisão europeia de arresto de contas	√	√	e-SENS
Registo dos testamentos	√	√	e-SENS
Citação ou notificação dos atos	√	√	e-CODEX