DÉCISION D'EXÉCUTION (UE) 2022/2519 DE LA COMMISSION

du 20 décembre 2022

relative aux spécifications et normes techniques applicables au système e-CODEX, y compris pour la sécurité et les méthodes de vérification de l'intégrité et de l'authenticité

(Texte présentant de l'intérêt pour l'EEE)

LA COMMISSION EUROPÉENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-CODEX), et modifiant le règlement (UE) 2018/1726 ([1]), et notamment son article 6, paragraphe 1, point a),

considérant ce qui suit:

(1) Conformément à l'article 5 du règlement (UE) 2022/850, le système e-CODEX se compose d'un point d'accès e-CODEX, de normes de procédure numériques et des produits logiciels, documentation et ressources de support dont la liste figure en annexe dudit règlement.

(2) Le point d'accès e-CODEX se compose d'une passerelle constituée d'un logiciel, fondé sur un ensemble commun de protocoles, permettant l'échange sécurisé d'informations sur un réseau de télécommunications avec d'autres passerelles utilisant le même ensemble commun de protocoles et d'un connecteur permettant de relier des systèmes connectés à la passerelle et consistant en un logiciel, fondé sur un ensemble commun de protocoles ouverts.

(3) Pour le bon déroulement du processus de cession du système e-CODEX et de sa reprise par l'eu-LISA, et afin de permettre l'accomplissement des tâches qui incombent à l'eu-LISA, il convient d'établir les spécifications et normes techniques minimales, y compris pour la sécurité et les méthodes de vérification de l'intégrité et de l'authenticité, qui sous-tendent les composants du système e-CODEX.

(4) Conformément aux articles 1er et 2 du protocole no 22 sur la position du Danemark annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, le Danemark n'a pas participé à l'adoption du règlement (UE) 2022/850 et n'est dès lors pas lié par la présente décision ni soumis à son application.

(5) Conformément aux articles 1er et 2 ainsi qu'à l'article 4 *bis*, paragraphe 1, du protocole no 21 sur la position du Royaume-Uni et de l'Irlande à l'égard de l'espace de liberté, de sécurité et de justice, annexé au traité sur l'Union européenne et au traité sur le fonctionnement de l'Union européenne, et sans préjudice de l'article 4 dudit protocole, l'Irlande n'a pas participé à l'adoption du règlement (UE) 2022/850 et n'est donc pas liée par la présente décision ni soumise à son application.

(6) Le Contrôleur européen de la protection des données a été consulté conformément à l'article 42, paragraphe 1, du règlement (UE) 2018/1725 du Parlement européen et du Conseil ([2]) et a rendu un avis le 24 novembre 2022.

(7) Les mesures prévues dans la présente décision sont conformes à l'avis du comité institué par l'article 19, paragraphe 1, du règlement (UE) 2022/850,

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

([2]) Règlement (UE) 2018/1725 du Parlement européen et du Conseil du 23 octobre 2018 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les institutions, organes et organismes de l'Union et à la libre circulation de ces données, et abrogeant le règlement (CE) no 45/2001 et la décision no 1247/2002/CE (JO L 295 du 21.11.2018, p. 39).

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

Les spécifications et normes techniques minimales, y compris pour la sécurité et les méthodes de vérification de l'intégrité et de l'authenticité, qui sous-tendent les composants du système e-CODEX visés à l'article 5 du règlement (UE) 2022/850 figurent à l'annexe de la présente décision.

Article 2

La présente décision entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 20 décembre 2022.

Par la Commission
La présidente
Ursula VON DER LEYEN

ANNEXE

Les spécifications et normes techniques applicables au système e-CODEX, y compris pour la sécurité et les méthodes de vérification de l'intégrité et de l'authenticité

1. **INTRODUCTION**

La présente annexe définit les spécifications et normes techniques minimales applicables aux composants e-CODEX, y compris pour la sécurité et les méthodes de vérification de l'intégrité et de l'authenticité.

2. **COMPOSANTS du SYSTÈME e-CODEX**

2.1. Conformément à l'article 5 du règlement (UE) 2022/850 du Parlement européen et du Conseil ([1]), le système e-CODEX se compose:

a) d'un point d'accès e-CODEX, qui se compose:

i) d'une passerelle;

ii) d'un connecteur;

b) de normes de procédure numériques;

c) des produits logiciels, documentation et autres ressources de support dont la liste figure en annexe du règlement (UE) 2022/850:

i) du code source de la plateforme centrale de test;

ii) du code source de l'outil de gestion de la configuration;

iii) de Metadata Workbench;

iv) du vocabulaire de base e-Justice de l'Union;

v) de la documentation relative à l'architecture.

2.2. D'un point de vue fonctionnel, ces éléments sont divisés en deux catégories: la boîte à outils e-CODEX et les ressources e-CODEX pouvant être mises en œuvre.

2.3. **La boîte à outils e-CODEX se compose des éléments suivants:**

a) la documentation relative à l'architecture e-CODEX;

b) le code source de la suite logicielle du connecteur;

c) le code source de l'outil de gestion de la configuration;

d) le code source de la plateforme centrale de test;

e) une licence pour Metadata Workbench délivrée par un tiers;

f) le vocabulaire de base e-Justice de l'Union;

g) des normes de procédure numériques.

a) La documentation relative à l'architecture e-CODEX

La documentation relative à l'architecture est un ensemble de documents servant à fournir aux parties prenantes concernées des connaissances techniques et des informations sur le choix des normes que les autres ressources du système e-CODEX doivent respecter. Elle définit les exigences et les principes qui s'appliquent lors de la création d'une communication transfrontière interopérable en vue de faciliter l'échange électronique de données, qui comprennent tout contenu transmissible sous forme électronique. En outre, elle énumère les normes et méthodologies choisies sur lesquelles se fonde le système e-CODEX. L'architecture garantit l'autonomie du système e-CODEX.

b) Le code source de la suite logicielle du connecteur

Le code source de la suite logicielle du connecteur est utilisé pour créer les artefacts pouvant être mis en œuvre qui sont décrits au point 2.4.2.

([1]) Règlement (UE) 2022/850 du Parlement européen et du Conseil du 30 mai 2022 relatif à un système informatisé pour l'échange électronique transfrontière de données dans le domaine de la coopération judiciaire en matière civile et pénale (système e-Codex), et modifiant le règlement (UE) 2018/1726 (JO L 150 du 1.6.2022, p. 1).

c) L'outil de gestion de la configuration

L'outil de gestion de la configuration est un outil en ligne permettant de gérer les fichiers de configuration associés à la passerelle «eDelivery» et au connecteur et fournit un mode normalisé de gestion du processus de configuration. L'entité exploitant un point d'accès e-CODEX autorisé peut avoir accès à l'outil de gestion de la configuration par l'intermédiaire d'un portail disponible à l'échelle mondiale et charger ses données de configuration «eDelivery». Les données chargées doivent inclure les informations relatives à la configuration du réseau du point de terminaison de la passerelle, tous les certificats de sécurité nécessaires à la connexion, ainsi que les projets, environnements et cas d'utilisation spécifiques auxquels l'entité participe. L'outil de gestion de la configuration vérifie automatiquement la validité des données chargées et, lorsque des erreurs sont constatées, il doit fournir un retour d'information à l'entité exploitant les points d'accès e-CODEX autorisés.

Lorsqu'une quelconque modification des données fournies par une entité exploitant un point d'accès e-CODEX autorisé est notifiée, un nouveau paquet de configuration e-CODEX (voir point 2.4.3) doit être généré à l'aide de cet outil. Toutes les entités exploitant des points d'accès e-CODEX autorisés doivent être informées de la création du nouveau paquet de configuration e-CODEX et peuvent le télécharger directement et à tout moment à partir de l'outil de gestion de la configuration. L'outil de gestion de la configuration peut fournir des paquets de configuration e-CODEX pour divers environnements informatiques, notamment TEST, ACCEPTANCE ou PRODUCTION.

Les nouveaux paquets de configuration e-CODEX doivent entrer en vigueur sept jours après leur création et, le cas échéant, les entités exploitant des points d'accès e-CODEX autorisés sont tenues d'installer le nouveau paquet dans leur environnement dans ce délai.

L'outil de gestion de la configuration tient également les entités exploitant les points d'accès e-CODEX autorisés informées des environnements d'exécution (runtimes) de ses certificats de sécurité et informe à l'avance, par courrier électronique, les points d'accès e-CODEX autorisés de l'expiration prochaine de leur certificat. Si une entité exploitant un point d'accès e-CODEX autorisé laisse expirer ses certificats de sécurité, ceux-ci doivent être automatiquement retirés lors de la création du paquet suivant.

L'outil de gestion de la configuration doit être hébergé au niveau central et être accessible 24 heures sur 24 et 7 jours sur 7 aux participants à e-CODEX. L'assistance doit être disponible uniquement durant les heures de bureau.

d) La plateforme centrale de test

La plateforme centrale de test d'e-CODEX est une infrastructure de test automatisée. Elle permet à l'entité exploitant un point d'accès e-CODEX autorisé de réaliser des tests de connectivité et des tests de bout en bout entre son infrastructure e-CODEX et un point de test central fixe sans qu'il soit nécessaire d'associer un autre partenaire (par exemple, un autre point d'accès e-CODEX autorisé) pour tester les fonctionnalités de communication. Elle permet de transmettre et de recevoir des messages de test personnalisables et réduit ainsi l'effort nécessaire pour tester une infrastructure e-CODEX à la fois dans le cadre des tests effectués lors de l'installation initiale et des tests de régression. La progression des messages individuels, les registres de preuve et d'erreurs relatifs au courrier électronique enregistré de l'Institut européen de normalisation des télécommunications (ETSI) sont suivis et présentés aux entités exploitant des points d'accès e-CODEX autorisés au moyen de processus visuels spécialement conçus.

La plateforme centrale de test se compose d'une passerelle e-CODEX, d'un connecteur, d'un connecteur-client et d'une interface utilisateur graphique web associée (actuellement une interface web frontale/dorsale web basée sur Nuxt.js) qui peuvent être utilisés pour envoyer des messages à la passerelle d'un partenaire ainsi que pour visualiser les messages qui sont envoyés à la plateforme centrale de test par la même passerelle. La plateforme centrale de test stocke actuellement d'importantes informations opérationnelles (variables locales) auprès d'une instance MongoDB et lit les informations relatives à la configuration (partie) à partir de la base de données des connecteurs. En outre, elle utilise l'interface de programmation d'application (API) du transfert d'état représentatif (REST) connecteur-client pour extraire des informations sur les messages e-CODEX et soumettre de nouveaux messages au connecteur et à la passerelle.

Afin de fournir une solution personnalisable pour chaque environnement e-CODEX, la plateforme centrale de test est déployée dans différentes instances (copies) qui existent dans différents environnements e-CODEX. Chaque instance de la plateforme centrale de test est actuellement déployée dans un environnement UNIX (CentOS 7), où tous les composants coexistent. Cela facilite la gestion et l'accès au système de fichiers tout en permettant que des adaptations soient apportées afin de tenir compte des installations dans lesquelles l'infrastructure de messagerie e-CODEX est séparée.

Chaque utilisateur de la plateforme centrale de test est relié à une (1) passerelle. Dans le cadre de l'utilisation de la plateforme centrale de test à des fins de test, la seule exigence est que la passerelle de ce point d'accès e-CODEX autorisé existe dans les modes-P pour cet environnement spécifique de l'outil de gestion de la configuration d'e-CODEX.

e) Metadata Workbench

Metadata Workbench est un outil de gestion du vocabulaire de base e-Justice de l'Union. Il permet aux modélisateurs sémantiques de maintenir le vocabulaire de manière durable en respectant la norme de modélisation des spécifications techniques des composants de base telle que définie dans la documentation relative à l'architecture e-CODEX. Il s'agit d'une solution de logiciel-service (SaaS) fondée sur le web dont l'accès est limité aux seulsdministrateurs du vocabulaire de base e-Justice de l'Union. Metadata Workbench est mis au point et exploité pour le compte du ministère de la justice et de la sécurité des Pays-Bas. Sur la base d'un accord de licence à conclure entre le ministère de la justice et de la sécurité et l'eu-LISA, l'eu-LISA se verra accorder l'accès à Metadata Workbench afin de gérer et d'exploiter le vocabulaire de base e-Justice de l'Union.

f) Le vocabulaire de base e-Justice de l'Union

Le vocabulaire de base e-Justice de l'Union est une ressource pour les termes et définitions sémantiques réutilisables à laquelle il est fait appel pour garantir la cohérence et la qualité des données dans le temps et entre les cas d'utilisation. Toutes les structures de messages spécifiques aux cas d'utilisation (schémas XML) sont fondées sur son répertoire sémantique.

Les évolutions futures du vocabulaire de base de e-Justice pourraient se faire dans le respect des vocabulaires de base ([2]). Afin de valider la conformité avec la spécification, un validateur XML pourrait être mis en place en utilisant le service de banc d'essai en matière d'interopérabilité proposé par la Commission.

g) Normes de procédure numériques

On entend par «norme de procédure numérique» les spécifications techniques relatives aux modèles de processus opérationnel et aux schémas de données qui énoncent la structure électronique des données échangées par l'intermédiaire du système e-CODEX, fondées sur le vocabulaire de base e-Justice de l'Union. Le modèle de processus opérationnel décrit la mise en œuvre technique de la procédure électronique de l'instrument juridique qui est pris en charge par le système e-CODEX.

Le modèle de processus opérationnel et le vocabulaire de base e-Justice de l'Union donnent lieu à des schémas XML décrivant la structure électronique des normes de procédure numériques. Les schémas XML permettent aux points d'accès autorisés d'envoyer et de recevoir des documents conformément à un instrument de coopération judiciaire transfrontière.

2.4. **Les ressources e-CODEX pouvant être mises en œuvre**

Les ressources e-CODEX pouvant être mise en œuvre sont des composants e-CODEX mis en œuvre par des entités exploitant un point d'accès e-CODEX autorisé dans leur environnement e-CODEX. À l'exception de la passerelle, elles doivent être distribuées par l'eu-LISA aux entités exploitant un point d'accès e-CODEX autorisé.

Les ressources pouvant être mise en œuvre sont les suivantes:

a) la passerelle (point 2.4.1);

b) la suite logicielle du connecteur (point 2.4.2);

c) le paquet de configuration e-CODEX (y compris les modes-P, les certificats publics et les paramètres de sécurité) (point 2.4.3);

d) l'architecture de la collaboration opérationnelle ou le modèle de processus dans le cadre des normes de procédure numériques;

e) les schémas XML, qui sont des structures de message dans le cadre des normes de procédure numériques.

2.4.1. ***La passerelle***

Dans le cadre du système e-CODEX, la passerelle est le module responsable de l'échange de communication de base. Actuellement, une passerelle met en œuvre les normes suivantes:

a) la norme OASIS ([3]) ebMS 3.0: messages d'échange entre passerelles conformes à la norme ebXML. Cette norme définit la structure selon laquelle un en-tête de message doit être présenté pour être intelligible dans le cadre de l'infrastructure e-CODEX;

b) le profil de messagerie de la déclaration d'applicabilité OASIS 4 (AS4): il s'agit d'un profil de conformité de la spécification OASIS ebMS 3.0;

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

([3]) Organisation pour l'avancement des normes structurées de l'information.

c) le profil commun du profil AS4 d'eDelivery ([4]).

Toute solution passerelle répondant à ces exigences peut être utilisée.

2.4.2. ***La suite logicielle du connecteur***

Le connecteur est un composant de liaison permettant de connecter les applications nationales spécifiques des normes de procédure numériques aux normes de messagerie génériques de la passerelle. Ce composant ajoute donc les caractéristiques suivantes à la communication de base déjà mise en place par le composant passerelle:

a) **preuves ETSI-REM**: il s'agit de preuves générées par le connecteur dans un format XML signé. L'objectif de ces preuves est d'informer l'expéditeur d'un message que le traitement du message a pu ou non être effectué. Les preuves sont générées et soumises par le connecteur à différentes étapes du traitement des messages;

b) **jeton TrustOK**: le connecteur émetteur valide l'intégrité et l'authentification du document (*business document*) contenu dans le message. Le résultat de cette validation est écrit dans le jeton TrustOK. Ce jeton est généré par un sous-module du connecteur: la bibliothèque de sécurité;

c) **conteneur ASIC-S**: conformément à la norme ETSI EN 319 162-1 relative aux signatures et aux infrastructures électroniques et aux conteneurs de signature y afférents (ASiC). Le conteneur garantit l'authenticité et l'intégrité de la charge utile transmise par le connecteur;

d) **sécurité WS**: afin de renforcer la sécurité de transmission des messages, le connecteur utilise, lors de la transmission, la sécurité WS au niveau de la passerelle ainsi qu'au niveau du système connecté. Cela signifie que chaque message transmis ou reçu par le connecteur est crypté et signé;

e) **API commune**: le connecteur offre une API stable qui définit les services web utilisés pour se connecter à la passerelle et à l'(aux) application(s) des systèmes connectés. La structure des messages échangés avec le connecteur est également décrite dans l'API du connecteur.

Outre le logiciel du connecteur lui-même, la suite contient également une application client destinée à supporter ou à remplacer un système connecté pour le traitement de la messagerie e-CODEX.

En outre, un plug-in a été développé spécialement pour la passerelle Domibus ([5]), afin de relier l'API commune du connecteur au cœur de traitement de la passerelle.

2.4.3. ***Le paquet de configuration e-CODEX***

Dans la communication fondée sur ebMS 3.0, un mode-P (ou mode de traitement) régit la transmission de tous les messages dans le cadre d'un échange de messages entre deux gestionnaires de services de messagerie. Un paquet de configuration e-CODEX comprend un ensemble de paramètres de configuration de messagerie (fichiers mode-P, plusieurs magasins de confiance pour les certificats, adresses réseau) qui précisent en détail les modalités d'envoi des messages.

Les paramètres de configuration d'envoi de messages peuvent être classés dans les cinq catégories suivantes:

a) paramètres relatifs à l'expéditeur, notamment:

   i) l'identifiant de la partie expéditrice;

   ii) le certificat utilisé par l'expéditeur pour signer les messages;

   iii) les autorités de certification auxquelles l'expéditeur fait confiance;

   iv) l'adresse (ou les adresses) du réseau à partir de laquelle (desquelles) l'expéditeur démarrera la communication;

b) paramètres relatifs au destinataire, notamment:

   i) l'identifiant de la partie destinataire;

   ii) le certificat dont l'utilisation est attendue par le destinataire pour crypter les messages;

   iii) les autorités de certification auxquelles le destinataire fait confiance;

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

([5]) La passerelle Domibus est gérée par la Commission (https://ec.europa.eu/digital-building-blocks/wikis/display/DIGITAL/Domibus).

iv) l'adresse (ou les adresses) du réseau à partir de laquelle (desquelles) le destinataire acceptera les communications entrantes;

c) paramètres relatifs à la paire expéditeur/destinataire, notamment (le cas échéant):

i) l'identifiant de l'accord, identifiant du mode-P;

d) paramètres relatifs aux normes de procédure numériques, notamment:

i) fonction(s) de la partie expéditrice;

ii) fonction(s) de la partie destinataire;

iii) service(s);

iv) actions(s) au sein du service;

e) paramètres relatifs à l'utilisation du protocole de messagerie ou du profil du protocole de messagerie.

Dans e-CODEX, tous les fichiers de configuration concernant un gestionnaire de services de messagerie ou un domaine sont regroupés dans un fichier principal qui peut être utilisé pour la configurer la passerelle et le connecteur.

Le fichier principal définit un réseau de communication individuel auquel le gestionnaire de services de messagerie peut recourir durant son fonctionnement. Il est nécessaire que la configuration soit effectuée de manière centralisée car toutes les informations de tous les points d'accès e-CODEX autorisés doivent être disponibles pour générer le paquet de configuration e-CODEX, qui est créé par l'outil de gestion de la configuration.

3. SÉCURITÉ ET MÉTHODES DE VÉRIFICATION DE L'INTÉGRITÉ ET DE L'AUTHENTICITÉ DU SYSTÈME E-CODEX

Le système e-CODEX est un système de communication qui apporte un soutien important en vue de satisfaire aux exigences en matière de sécurité et de protection des données. En particulier, le système e-CODEX fournit les caractéristiques techniques nécessaires pour satisfaire à toutes les exigences prévues par le règlement (UE) n° 910/2014 du Parlement européen et du Conseil ([6]).

3.1. Sécurité dès la conception

Le système e-CODEX est, d'un point de vue technique, un mécanisme de transport. Il existe différentes couches pertinentes en matière de sécurité:

a) une couche réseau;

b) une couche de transport;

c) une couche de message;

d) une couche du document.

Des mesures de sécurité sont appliquées à chacune de ces couches.

3.1.1. *Couche réseau*

e-CODEX peut être utilisé avec différents types de couches réseau. La couche réseau est généralement utilisée dans le cadre de connexions internet normales. La sécurité est donc conforme aux applications de sécurité habituelles de la technologie internet (et est renforcée par les autres couches décrites au présent point). Cette couche réseau suffit dans la plupart des cas d'utilisation d'e-CODEX. Pour des exigences de sécurité plus élevées, une couche réseau supplémentaire peut également être utilisée. D'autres réseaux peuvent également être pris en considération.

3.1.2. *Couche de transport*

La couche de transport est généralement protégée par le protocole de sécurité de la couche de transport (TLS) ou mTLS (TLS mutuel). Il s'agit d'une norme bien établie aux fins de la protection de la couche de transport dans les technologies internet et utilisée dans le monde entier dans un grand nombre de services. Le protocole TLS/mTLS prévoit le cryptage et l'authentification au niveau du canal de transport. Il garantit l'itinéraire de transport entre chaque pôle de l'itinéraire de transport. Chaque pôle doit décrypter (uniquement) les données relatives à l'adresse pour transmettre le message au pôle suivant. Avant de les transmettre, chaque pôle crypte à nouveau les données relatives à l'adresse. L'application d'un protocole TLS simple (à sens unique) est possible et encore parfois observée, mais il est recommandé d'appliquer un protocole TLS à double sens (mTLS), qui s'impose de plus en plus comme la norme en vigueur en matière de protection de la couche de transport.

([6]) Règlement (UE) n° 910/2014 du Parlement européen et du Conseil du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur et abrogeant la directive 1999/93/CE (JO L 257 du 28.8.2014, p. 73).

3.1.3. ***Couche de message***

Au niveau de la couche de message, plusieurs normes sont appliquées par différents composants e-CODEX:

a) le protocole utilisé aux fins de la transmission entre passerelles (en tant que couche de message) est le protocole AS4, qui signe et crypte les messages en fonction de la configuration de sécurité au niveau de la passerelle;

b) le composant principal du système e-CODEX est le connecteur. Il renforce la sécurité au niveau de la couche de message en utilisant sécurité WS pour signer et crypter les messages en ce qui concerne les services web vers la passerelle et l'arrière-plan ou les arrière-plans. Par conséquent, un cryptage de connecteur à connecteur est appliqué en sus;

c) des certificats numériques sont utilisés dans l'ensemble des systèmes e-CODEX pour les fonctionnalités de signature et de cryptage. Ces certificats numériques de cryptage et de signature sont conformes à la norme X.509.

3.1.4. ***Couche du document***

Les messages contiennent des documents et des pièces jointes. Ceux-ci sont contenus dans un paquet dénommé «conteneur». Le conteneur est construit selon la norme ASIC-S. Le connecteur expéditeur signe le conteneur ASIC-S et la signature est validée dès réception par le connecteur destinataire.

3.2. **Méthodes de vérification de l'intégrité et de l'authenticité**

3.2.1. ***Accès à la configuration e-CODEX***

La communication entre les points d'accès e-CODEX doit faire l'objet d'une configuration préalable. Cette configuration s'effectue au moyen d'un paquet de configuration e-CODEX. Le paquet de configuration contient les données d'adressage, la politique de sécurité appliquée et d'autres informations. Il contient en outre les magasins de confiance accompagnés des certificats publics de tous les points d'accès e-CODEX participants. Les fichiers de configuration sont créés pour la configuration de chaque partenaire par un «coordinateur central pour la configuration» à l'aide de l'outil de gestion de la configuration. L'accès à cet outil de gestion de la configuration est limité aux partenaires et accordé à chacun d'entre eux uniquement sur demande personnelle et individuelle. L'accès administratif est limité aux coordinateurs pour la configuration et doit être géré par l'eu-LISA.

3.2.2. ***Signatures et cachets électroniques pris en charge***

Le système e-CODEX doit prendre en charge tous les types de cachets électroniques et de signatures électroniques prévus par le règlement (UE) nº 910/2014.

3.2.3. ***Jeton TrustOK d'e-CODEX***

Le connecteur expéditeur valide la signature de la norme de procédure numérique d'un message. Le résultat de cette validation est écrit dans le jeton TrustOK d'e-CODEX. Ce jeton est généré par une bibliothèque de sécurité, qui est un sous-module du connecteur. La validation de la signature électronique est effectuée par le connecteur e-CODEX à l'aide d'outils DSS (service de signature numérique).

3.2.4. ***Jeton lisible par voie électronique (XML)***

Le jeton lisible par voie électronique se présente sous la forme d'un fichier XML sous-jacent à un schéma donné contenant toutes les informations relatives à la signature du jeton relatif au message (*business token*) et le rapport de validation résultant de la validation juridique et technique.

3.2.5. ***Jeton lisible par l'homme (PDF)***

Le fichier PDF se compose de trois parties. La première partie présentée sur la première page du jeton proprement dit contient des informations générales sur le système électronique avancé et une évaluation de la validité juridique du document (*business document*) contenu dans le message. En outre, une clause de non-responsabilité et un «cachet de validation» indiquant le résultat de la validation juridique (positif/négatif) figurent au bas de la page.

Un système électronique avancé est un système connecté capable d'identifier l'utilisateur en toute sécurité et d'assurer l'intégrité des messages transmis à travers lui entre le client et le connecteur e-CODEX.

La deuxième partie de la deuxième page fournit une vue d'ensemble technique normalisée des informations contenues dans le rapport de validation original. Les informations fournies par la vue d'ensemble technique varient selon le système connecté utilisé (authentification ou signature). Un jeton fondé sur la signature contient les informations fournies par le certificat sous-jacent, notamment les attributs (le cas échéant). Un jeton fondé sur l'authentification contient le nom de l'institution émettrice du document et, lorsqu'il est fourni, le nom de l'auteur du document.

Au bas de cette page se trouvent un cachet dans la couleur du résultat de la validation technique des documents (vert/jaune/rouge) ainsi qu'une une brève description, par exemple des informations supplémentaires sur les raisons pour lesquelles un document a fait l'objet d'une évaluation technique jaune.

La troisième partie du document est constituée du rapport de validation original tel qu'il a été créé par le logiciel de validation de l'État membre émetteur.

4. **NORMES DE PROCÉDURE NUMÉRIQUES MISES AU POINT À CE JOUR**

E-justice pour la signification ou la notification des actes	NORME DE PROCÉDURE NUMÉRIQUE: modèle de processus	NORME DE PROCÉDURE NUMÉRIQUE: schéma XML	Source du projet
Injonction de payer européenne	√	√	e-CODEX
Petits litiges	√	√	e-CODEX
Mandat d'arrêt européen	√	√	e-CODEX
Sanctions pécuniaires	√	√	e-CODEX
Entraide judiciaire en matière pénale	√	√	e-CODEX
DC 909 (peines privatives de liberté)	√	√	e-CODEX
Affaires matrimoniales	√	√	e-SENS
Ordonnance de l'UE de saisie conservatoire des comptes bancaires	√	√	e-SENS
Registre des testaments	√	√	e-SENS
Signification et notification de documents	√	√	e-CODEX