Journal officiel
de l'Union européenne

FR
Série L

2025/1550

29.7.2025

RÈGLEMENT D'EXÉCUTION (UE) 2025/1550 DE LA COMMISSION

du 28 juillet 2025

établissant les spécifications et autres exigences techniques pour le système informatique décentralisé visées par le règlement (UE) 2023/1543 du Parlement européen et du Conseil

LA COMMISSION EUROPÉENNE,

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

vu le règlement (UE) 2023/1543 du Parlement européen et du Conseil du 12 juillet 2023 relatif aux injonctions européennes de production et aux injonctions européennes de conservation concernant les preuves électroniques dans le cadre des procédures pénales et aux fins de l'exécution de peines privatives de liberté prononcées à l'issue d'une procédure pénale ([1]), et notamment son article 25, paragraphe 1, points a), b), c) et d),

considérant ce qui suit:

(1) Afin de mettre en place le système informatique décentralisé visé par le règlement (UE) 2023/1543, il est nécessaire de définir et d'adopter des spécifications, mesures et objectifs techniques pour la mise en œuvre de ce système.

(2) Conformément au règlement (UE) 2023/1543, le système informatique décentralisé devrait comprendre les systèmes informatiques des États membres et des agences et organes de l'Union, ainsi que des points d'accès e-CODEX interopérables, par l'intermédiaire desquels ces systèmes informatiques sont interconnectés. Par conséquent, les spécifications et autres exigences techniques du système informatique décentralisé devraient refléter ce cadre.

(3) Conformément au règlement (UE) 2023/1543, les points d'accès du système informatique décentralisé devraient se fonder sur les points d'accès e-CODEX autorisés tels que définis à l'article 3, paragraphe 3, du règlement (UE) 2022/850 du Parlement européen et du Conseil ([2]).

(4) Les États membres peuvent choisir d'utiliser le logiciel de mise en œuvre de référence développé par la Commission comme système dorsal en lieu et place d'un système informatique national. Afin de garantir l'interopérabilité, tant les systèmes informatiques nationaux que le logiciel de mise en œuvre de référence devraient être soumis aux mêmes spécifications et exigences techniques établies dans le présent règlement.

(5) Afin d'atténuer les problèmes techniques potentiels liés à la capacité et à la fiabilité du système informatique décentralisé, il est nécessaire de fixer un seuil pour le volume de preuves électroniques transmises par l'intermédiaire de ce système. Après le lancement du système, la fréquence et le volume de ces transmissions devraient faire l'objet d'un suivi et le seuil devrait être ajusté, s'il y a lieu, afin de maximiser l'efficacité du système.

(6) Afin de renforcer l'interopérabilité et l'efficacité du système informatique décentralisé, il convient de rendre obligatoire l'utilisation de normes ETSI appropriées. Les évolutions futures devraient faire l'objet d'un suivi et, le cas échéant, l'adoption de normes ETSI supplémentaires devrait être envisagée.

(7) L'Irlande est liée par le règlement (UE) 2023/1543 et participe donc à l'adoption du présent règlement.

(8) 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'est pas lié par l'application du présent règlement, ni soumis à celle-ci.

([1]) JO L 191 du 28.7.2023, p. 118, ELI: http://data.europa.eu/eli/reg/2023/1543/oj.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2022/850/oj).

(9) 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 ([3]) et a rendu un avis le 25 juin 2025.

(10) Les mesures prévues par le présent règlement sont conformes à l'avis du comité créé par l'article 26 du règlement (UE) 2023/1543,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

Spécifications techniques du système informatique décentralisé

Les spécifications et exigences, mesures et objectifs techniques du système informatique décentralisé visés à l'article 25, paragraphe 1, du règlement (UE) 2023/1543 pour la communication au sens de l'article 19 dudit règlement, sont définis à l'annexe du présent règlement.

Article 2

Entrée en vigueur

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans les États membres conformément aux traités.

Fait à Bruxelles, le 28 juillet 2025.

Par la Commission
La présidente
Ursula VON DER LEYEN

([3]) 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) n° 45/2001 et la décision n° 1247/2002/CE (JO L 295 du 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

ANNEXE

SPÉCIFICATIONS TECHNIQUES DU SYSTÈME INFORMATIQUE DÉCENTRALISÉ

(visées à l'article 1er)

1. Introduction et champ d'application

La présente annexe énonce les spécifications, mesures et objectifs techniques du système informatique décentralisé pour les procédures prévues par le règlement (UE) 2023/1543.

Au titre du règlement (UE) 2023/1543, et en particulier de son article 19, le système informatique décentralisé doit permettre la communication écrite entre les autorités compétentes et les établissements désignés ou les représentants légaux, entre les autorités compétentes, ainsi qu'entre les autorités compétentes et les agences ou organes compétents de l'Union.

2. Définitions

2.1. On entend par «HyperText Transfer Protocol Secure» ou «HTTPS» (protocole de transfert hypertexte sécurisé): les canaux de communication cryptée et de connexion sécurisée;

2.2. «non-répudiation de l'origine»: les mesures apportant la preuve de l'intégrité et la preuve de l'origine des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique ainsi que les signatures et cachets électroniques;

2.3. «non-répudiation de la réception»: les mesures apportant à l'émetteur la preuve de la réception des données par le destinataire prévu des données grâce à des méthodes telles que la certification numérique, l'infrastructure à clé publique ainsi que les signatures et cachets électroniques;

2.4. «Simple Object Access Protocol (SOAP)»: selon les normes du World Wide Web Consortium, une spécification de protocole de messagerie pour l'échange d'informations structurées dans la mise en œuvre de services web dans les réseaux informatiques;

2.5. «Representational State Transfer (REST)»: un style d'architecture permettant de concevoir des applications en réseau, reposant sur un modèle de communication client-serveur sans état et utilisant des méthodes standards pour effectuer des opérations sur des ressources, qui sont généralement représentées dans des formats structurés;

2.6. «service web»: un logiciel destiné à assurer une interaction interopérable machine-machine sur un réseau et qui dispose d'une interface décrite sous un format pouvant être traité par machine;

2.7. «échange de données»: l'échange de messages, de formulaires, de documents et de preuves électroniques par l'intermédiaire du système informatique décentralisé;

2.8. «API»: une interface de programmation d'application fondée sur une norme commune d'échange de données, permettant aux fournisseurs de services qui utilisent des solutions informatiques sur mesure aux fins de l'échange d'informations et de données liées aux demandes de preuves électroniques d'accéder aux systèmes informatiques décentralisés par des moyens automatisés;

2.9. «interface web», une interface utilisateur disponible sur l'internet via HTTPS, qui permet aux fournisseurs de services d'accéder manuellement au système informatique décentralisé afin de communiquer en toute sécurité avec les autorités et d'échanger des informations et des données liées aux demandes de preuves électroniques, sans avoir à mettre en place leur propre infrastructure spécifique;

2.10. «normes ETSI»: les spécifications et les normes techniques élaborées par l'Institut européen de normalisation des télécommunications (ETSI) afin d'assurer l'interopérabilité, la sécurité et l'efficacité des technologies de l'information et de la communication. Elles fournissent des cadres, des protocoles et de bonnes pratiques pour un large éventail de technologies, y compris les réseaux mobiles, les communications radio, la cybersécurité et l'infrastructure internet;

2.11. «valeur de hachage»: une sortie de longueur fixe générée par une fonction de hachage cryptographique lorsqu'elle est appliquée à une entrée de longueur arbitraire. Une fonction de hachage cryptographique est conçue pour satisfaire aux propriétés fondamentales de sécurité, notamment la résistance à la préimage, la résistance à la seconde préimage et la résistance à la collision, en assurant une solidité contre l'inversion et les attaques de collision;

2.12. «système e-CODEX»: le système e-CODEX tel qu'il est défini à l'article 3, paragraphe 1, du règlement (UE) 2022/850;

2.13. «vocabulaire de base e-Justice de l'Union»: le vocabulaire de base e-Justice de l'Union tel que défini au point 4 de l'annexe du règlement (UE) 2022/850;

2.14. «ebMS»: le service de messagerie ebXML, un protocole de messagerie développé par OASIS qui permet un échange sécurisé, fiable et interopérable de documents commerciaux sur support électronique utilisant SOAP, favorisant l'intégration interentreprises dans divers systèmes;

2.15. «AS4»: la déclaration d'applicabilité 4, une norme OASIS qui définit le profil ebMS 3.0 et simplifie la messagerie interentreprises sécurisée et interopérable en utilisant des normes ouvertes telles que SOAP et WS-Security;

2.16. «durée maximale d'interruption admissible», le délai maximal acceptable pour rétablir le service après un incident;

2.17. «perte de données maximale admissible»: le volume maximal acceptable de perte de données en cas de défaillance.

3. **Méthodes de communication par voie électronique**

3.1. Aux fins de la communication écrite entre les autorités compétentes des États membres, entre les autorités compétentes et les établissements désignés ou les représentants légaux des fournisseurs de services, ainsi qu'entre les autorités compétentes et les agences ou organes de l'Union, le système informatique décentralisé utilise des méthodes de communication fondées sur des services, telles que les services web ou d'autres composants et solutions logicielles réutilisables à des fins d'échange de données. Plus précisément, il nécessitera une communication par l'intermédiaire des points d'accès e-CODEX, comme prévu à l'article 5, paragraphe 2, du règlement (UE) 2022/850. Par conséquent, pour garantir un échange transfrontière de données efficace et interopérable, le système informatique décentralisé facilite la communication par l'intermédiaire du système e-CODEX.

3.2. Compte tenu du volume élevé prévu de preuves électroniques à transmettre en vertu d'une injonction européenne de production au moyen du système informatique décentralisé, comme indiqué à l'article 19, paragraphes 1 et 4, du règlement (UE) 2023/1543, qui peut entraîner des contraintes en matière de capacité technique susceptibles d'avoir une incidence négative sur le système informatique décentralisé, les preuves électroniques sont transmises par l'intermédiaire de ce système dans la mesure où elles ne dépassent pas le seuil de 25 méga-octets (25 600 kilo-octets). La transmission des preuves électroniques dépassant le seuil s'effectue conformément à l'article 19, paragraphe 5, dudit règlement.

3.3. Vu l'article 19, paragraphe 6, du règlement (UE) 2023/1543, dans le cas où une transmission est effectuée par des moyens de substitution, comme le prévoit ledit paragraphe, en raison d'une impossibilité d'utiliser le système informatique décentralisé pour l'un des motifs énoncés à l'article 19, paragraphe 5, dudit règlement.

3.3.1. Lorsque la transmission concerne une communication écrite, y compris l'échange de formulaires, entre des autorités compétentes et des fournisseurs de services au sens de l'article 19, paragraphe 1, du règlement (UE) 2023/1543, l'autorité à l'origine de la transmission l'enregistre dans son système informatique national, qui fait partie du système informatique décentralisé. Les informations enregistrées comprennent au minimum un numéro de référence de l'affaire ou du dossier, sa date et son heure, l'expéditeur et le destinataire, le nom du fichier et sa taille.

3.3.2. Lorsque la transmission concerne une communication écrite, y compris l'échange de formulaires, entre autorités compétentes, ainsi qu'une communication écrite avec les agences ou organes compétents de l'Union au sens de l'article 19, paragraphe 4, du règlement (UE) 2023/1543, l'autorité à l'origine de la transmission l'enregistre dans le système informatique décentralisé, notamment dans son système informatique national ou, le cas échéant, dans les systèmes informatiques gérés par l'agence ou l'organe compétent de l'Union. Les informations enregistrées comprennent au minimum un numéro de référence de l'affaire ou du dossier, la date et l'heure de transmission, l'expéditeur et le destinataire, le nom du fichier et sa taille.

3.3.3. Lorsque des preuves électroniques produites en vertu d'une injonction européenne de production ont été transmises par d'autres moyens de communication entre des fournisseurs de services et les autorités compétentes de l'État d'émission ([1]), ou lorsque les preuves électroniques sont transmises par d'autres moyens de l'autorité chargée de la mise en œuvre aux autorités compétentes de l'État d'émission dans le cadre de la procédure de mise en œuvre prévue à l'article 16, paragraphe 9, du règlement (UE) 2023/1543, l'autorité à l'origine de la transmission:

a) enregistre et transmet à l'autorité à laquelle les preuves électroniques ont été transmises ou mises à disposition les informations suivantes dans le cadre d'un manifeste:

1) des informations sur l'expéditeur et le destinataire;

2) des métadonnées associant les preuves électroniques fournies à une ou plusieurs injonction(s) européenne(s) de production ou de conservation particulière(s);

3) la date et l'heure de la transmission ou l'indication de la date à laquelle les preuves électroniques ont été mises à la disposition du destinataire;

4) des informations concernant les moyens de transmission [par exemple un enregistrement du lien sécurisé par lequel les preuves électroniques ont été mises à disposition, un accusé de réception ou une preuve de livraison provenant des services postaux, etc. ([2])];

5) le(s) nom(s) complet(s) du(es) fichier(s) des preuves électroniques transmises ou autrement mises à la disposition du destinataire prévu résidant dans l'État d'émission;

6) le volume des données des preuves électroniques transmises ou autrement mises à la disposition du destinataire prévu résidant dans l'État d'émission;

7) au moins une valeur de hachage des données qui ont été transmises ou mises à disposition, et une indication du ou des algorithmes de hachage utilisés. Le ou les algorithmes de hachage utilisés pour le calcul de cette ou de ces valeurs de hachage sont des algorithmes cryptographiquement forts, couramment utilisés, et non sujets à des faiblesses publiées telles que les collisions (par exemple SHA-512, SHA3-512, BLAKE2 ou RIPEMD-160, mais potentiellement plus solides, en fonction des évolutions technologiques);

b) le cas échéant, indique, dans le cadre du manifeste visé au point a) ci-dessus, la date et l'heure jusqu'auxquelles les preuves électroniques demeureront accessibles. Cette échéance permet à l'autorité compétente de l'État d'émission de disposer d'un délai raisonnable pour récupérer les preuves électroniques, qui ne peut être inférieur à 10 jours calendaires ni supérieur à 45 jours calendaires à compter du moment où les preuves électroniques sont mises à disposition. À la demande de l'autorité compétente de l'État d'émission, le délai indiqué par l'autorité à l'origine de la transmission peut être prolongé dans un cas particulier;

c) peut enregistrer et transmettre toute information ou remarque complémentaire pertinente en l'espèce à l'autorité à laquelle les preuves électroniques ont été transmises ou mises à disposition, dans le cadre du manifeste visé au point a) ci-dessus.

3.4. Vu l'article 28 du règlement (UE) 2023/1543, le logiciel de mise en œuvre de référence recueille, transmet ou donne accès, au moyen de programmes, aux statistiques visées au paragraphe 2 dudit article dans des formats de données structurés (XML, par exemple) et non structurés (PDF, par exemple). Conformément à l'article 28, paragraphe 3, du règlement (UE) 2023/1543, lorsqu'ils sont équipés techniquement, les portails nationaux ([3]) gérés par les États membres peuvent également transmettre ou fournir ces statistiques à la Commission au moyen d'un processus automatisé. La Commission publie des orientations sur la structure des données et la méthode de collecte et de communication de ces statistiques.

([1]) Par souci de clarté, les références aux autorités nationales compétentes s'entendent également, mutatis mutandis, comme s'appliquant aux membres nationaux d'Eurojust, aux procureurs européens et aux procureurs européens délégués, dans la mesure où ils sont habilités à exercer les mêmes fonctions en vertu du droit de l'Union et du droit national.

([2]) Il convient de rappeler que, conformément à l'article 19, paragraphe 5, la transmission par ces moyens de communication de substitution répond aux exigences de rapidité, de sécurité et de fiabilité permettant au destinataire d'en établir l'authenticité.

([3]) Par «portails nationaux», on entend les «systèmes informatiques» nationaux qui font partie du système informatique décentralisé, tels que définis à l'article 3, paragraphe 21, du règlement (UE) 2023/1543.

4. **Protocoles de communication**

4.1. Le système informatique décentralisé utilise des protocoles internet sécurisés pour:

a) la communication au sein du système informatique décentralisé entre les autorités compétentes;

b) la communication au sein du système informatique décentralisé entre les autorités compétentes et les agences et organes de l'Union;

c) la communication entre les autorités compétentes et les fournisseurs de services au moyen d'une API et de l'interface web; et

d) la communication avec la base de données des cours et tribunaux.

4.2. Aux fins de la définition et de la transmission de données et de métadonnées structurées, les composants du système informatique décentralisé sont basés sur des normes et des protocoles sectoriels complets et largement acceptés, tels que SOAP et REST, notamment ceux référencés par les organisations européennes de normalisation, telles que l'ETSI.

4.3. Pour les protocoles de transport et de messagerie, le système informatique décentralisé repose sur des protocoles normalisés sécurisés tels que:

a) le profil AS4 pour l'échange transfrontière de données, garantissant une messagerie sécurisée et fiable avec chiffrement et non-répudiation;

b) les API HTTPS/RESTful pour la communication prenant en charge les formats JSON et XML;

c) SOAP pour les interactions de haute fiabilité, intégrant WS-Security pour l'authentification et le chiffrement.

4.4. Aux fins d'un échange de données fluide et interopérable, les protocoles de communication utilisés par le système informatique décentralisé sont conformes aux normes d'interopérabilité applicables.

4.5. Le cas échéant, les schémas XML pour les preuves électroniques utilisent les normes ou vocabulaires pertinents, qui sont nécessaires à la validation correcte des éléments et types définis dans le présent schéma. Cela peut inclure:

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

b) des types de données non qualifiées;

c) une liste de codes pour les codes linguistiques de l'Union européenne.

En outre, le cas échéant, les schémas XML peuvent intégrer des normes ETSI pertinentes pour utiliser leurs définitions.

4.6. La Commission définit les spécifications de l'API commune, que les États chargés de la mise en œuvre mettent à la disposition des fournisseurs de services pour leur permettre d'accéder au système informatique décentralisé. Dans la mesure du possible et dans la mesure où cela est raisonnable, la présente API est basée sur la norme ETSI TS 104 144 [«Interface definition for the e-Evidence Regulation (EU) 2023/1543 for National Authorities and Service Providers»].

4.7. En ce qui concerne les protocoles de sécurité et d'authentification, le système informatique décentralisé repose sur des protocoles normalisés tels que:

a) TLS (sécurité de la couche de transport) pour la communication cryptée et authentifiée sur les réseaux, qui prend en charge l'authentification mutuelle au moyen de certificats numériques X.509;

b) OAuth/OpenID Connect (OIDC) pour une authentification et une autorisation sécurisées;

c) Infrastructure à clé publique et signatures numériques pour l'échange sécurisé de clés et la vérification de l'intégrité des messages, au moyen de certificats numériques (X.509) délivrés par des autorités de certification reconnues (AC).

5. **Objectifs en matière de sécurité de l'information et mesures techniques pertinentes**

5.1. En ce qui l'échange d'informations au moyen du système informatique décentralisé, les mesures techniques permettant d'assurer le respect des normes minimales de sécurité informatique sont notamment les suivantes:

a) mesures visant à garantir la confidentialité des informations, y compris par le recours à des canaux de communication sécurisés;

b) mesures visant à garantir l'intégrité des données (messages, formulaires, documents et preuves électroniques) au repos et en transit;

c) mesures visant à garantir la non-répudiation de l'origine de l'émetteur des informations au sein du système informatique décentralisé et la non-répudiation de la réception des informations;

d) mesures visant à garantir la disponibilité en veillant à un accès continu aux services et aux données, en prévenant les perturbations dues aux cyberattaques ou aux défaillances;

e) mesures visant à garantir la journalisation des événements liés à la sécurité conformément aux recommandations internationales reconnues en matière de normes de sécurité informatique;

f) mesures visant à garantir l'authentification et l'autorisation et mesures visant à vérifier l'identité des systèmes connectés au système informatique décentralisé.

5.2. Les composants du système informatique décentralisé garantissent une communication et une transmission de données sécurisées, en utilisant le chiffrement, l'infrastructure à clé publique avec des certificats numériques d'authentification et l'échange sécurisé de clés, ainsi que des protocoles de messagerie sécurisée tels qu'AS4 (ebMS), les API RESTful et SOAP, afin de préserver la confidentialité et l'intégrité des messages.

5.3. Les composants du système informatique décentralisé sont développés conformément au principe de protection des données dès la conception et par défaut, et des mesures administratives, organisationnelles et techniques appropriées sont mises en œuvre pour garantir un niveau élevé de cybersécurité.

5.4. La Commission conçoit, développe et maintient le logiciel de mise en œuvre de référence conformément aux exigences et principes en matière de protection des données énoncés dans le règlement (UE) 2018/1725. Le logiciel de mise en œuvre de référence fourni par la Commission permet aux États membres de se conformer aux obligations qui leur incombent respectivement en vertu du règlement (UE) 2016/679 du Parlement européen et du Conseil ([4]) et de la directive (UE) 2016/680 du Parlement européen et du Conseil ([5]), selon le cas.

5.5. Les États membres qui utilisent un système informatique national différent du logiciel de mise en œuvre de référence mettent en œuvre les mesures nécessaires pour s'assurer qu'il est conforme aux exigences du règlement (UE) 2016/679 et de la directive (UE) 2016/680, selon le cas.

5.6. Eu égard à leur participation au système informatique décentralisé, Eurojust et le Parquet européen mettent en œuvre les mesures nécessaires afin de garantir que leurs systèmes informatiques respectifs sont conformes aux exigences du règlement (UE) 2018/1725 et de leurs actes fondateurs.

5.7. Les États membres, Eurojust et le Parquet européen mettent en place des mécanismes solides de détection des menaces et de réaction aux incidents afin de garantir l'identification, l'atténuation et le rétablissement en temps utile à la suite des incidents de sécurité, conformément à leurs politiques pertinentes, pour les systèmes informatiques faisant partie du système informatique décentralisé relevant de leur responsabilité.

6. **Chiffrement des preuves électroniques** ([6])

6.1. Sans préjudice des mesures de sécurité prévues par le système informatique décentralisé, lorsqu'elles émettent une injonction européenne de production, les autorités compétentes peuvent en outre fournir un certificat public spécifique X.509 pour le chiffrement asymétrique des preuves électroniques.

([4]) Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (JO L 119 du 4.5.2016, p. 1).

([5]) Directive (UE) 2016/680 du Parlement européen et du Conseil du 27 avril 2016 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel par les autorités compétentes à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, et à la libre circulation de ces données, et abrogeant la décision-cadre 2008/977/JAI du Conseil (JO L 119 du 4.5.2016, p. 89).

([6]) Pour éviter toute ambiguïté, le terme «preuves électroniques» se limite à la définition figurant à l'article 3, paragraphe 8, du règlement (UE) 2023/1543.

6.2. L'émission, la gestion, la vérification et tous les aspects connexes des certificats visés au point 6.1, ainsi que l'infrastructure à clé publique correspondante, relèvent de la seule responsabilité de l'État d'émission.

6.3. Sans préjudice des évolutions technologiques futures, les certificats publics prennent en charge des algorithmes de chiffrement standard, tels que l'algorithme RSA (Rivest-Shamir Adleman) ou l'ECDH (échange de clés Diffie-Hellman basé sur les courbes elliptiques) pour l'ECC (cryptographie par courbes elliptiques).

6.4. Les certificats publics contiennent l'extension «keyUsage» appropriée, telle que «keyEncipherment» ou «dataEncipherment» pour les certificats basés sur le RSA et «keyAgreement» pour les certificats basés sur l'ECC. Ils sont mis à disposition au format PEM [Privacy-Enhanced Mail (courrier électronique à confidentialité renforcée)] ou DER [Distingued Encoding Rules (règles de codage distinctes)].

6.5. Lorsque l'autorité d'émission a fourni un certificat public X.509, et qu'un fournisseur de services envoie les preuves électroniques produites en vertu d'une injonction européenne de production, le fournisseur, avant la transmission de ces données par l'intermédiaire du système informatique décentralisé, chiffre les preuves électroniques à l'aide du certificat public X.509 correspondant fourni par l'État d'émission.

6.6. Lorsque l'autorité émettrice a fourni un certificat public X.509, mais que la transmission de preuves électroniques sous forme chiffrée n'est pas possible pour des raisons techniques ou d'autres raisons justifiables, et sans préjudice de la disposition prévue à l'article 19, paragraphe 5, du règlement (UE) 2023/1543, le fournisseur de services peut transmettre les données sans chiffrer le contenu. Dans ce cas, le fournisseur de services fournit une explication motivée à l'autorité d'émission.

7. **Objectifs minimaux en matière de disponibilité**

7.1. Les États membres, Eurojust et le Parquet européen veillent à ce que les composants du système informatique décentralisé relevant de leur responsabilité soient disponibles 24 heures sur 24 et 7 jours sur 7, avec un taux cible de disponibilité technique d'au moins 98 % sur une base annuelle, à l'exclusion de la maintenance programmée.

7.2. La Commission veille à ce que la base de données des cours et tribunaux soit disponible 24 heures sur 24 et 7 jours sur 7, avec un taux de disponibilité technique cible de plus de 99 % sur une base annuelle, à l'exclusion de la maintenance programmée.

7.3. Dans la mesure du possible, pendant les jours ouvrables, les opérations de maintenance doivent être planifiées entre 20 h 00 et 7 h 00 HEC.

7.4. Les États membres, Eurojust et le Parquet européen informent la Commission et les autres États membres des activités de maintenance selon les modalités suivantes:

a) 5 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner jusqu'à 4 heures d'indisponibilité;

b) 10 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner entre 4 et 12 heures d'indisponibilité;

c) 30 jours ouvrables à l'avance en cas d'opérations de maintenance pouvant entraîner plus de 12 heures d'indisponibilité.

7.5. Lorsque les États membres, Eurojust ou le Parquet européen disposent de fenêtres de maintenance régulières fixes, ils informent la Commission et les participants au système informatique décentralisé de l'heure et du ou des jours où ces fenêtres régulières fixes sont prévues. Nonobstant les obligations énoncées au point 7.4, si des composants du système informatique décentralisé relevant de la responsabilité des États membres, d'Eurojust ou du Parquet européen deviennent indisponibles au cours d'une telle fenêtre fixe régulière, ceux-ci peuvent choisir de ne pas en informer la Commission à chaque fois.

7.6. En cas de défaillance technique imprévue des composants du système informatique décentralisé relevant de la responsabilité des États membres, d'Eurojust ou du Parquet européen, ceux-ci informent sans délai la Commission et les participants au système informatique décentralisé de cette défaillance et, s'il est connu, du délai de rétablissement prévu.

7.7. En cas d'activités de maintenance ou de défaillance technique imprévue de composants du système informatique décentralisé relevant de la responsabilité d'un État membre et ayant une incidence négative sur la disponibilité de l'API et/ou de l'interface web pour les fournisseurs de services, l'État membre concerné met rapidement cette information à disposition sur un site web et/ou la communique aux fournisseurs de services opérant sur son territoire, sans retard excessif.

7.8. En cas de défaillance technique inattendue de la base de données des cours et tribunaux, la Commission informe sans délai les États membres, Eurojust et le Parquet européen de cette indisponibilité et, si elle est connue, du délai de rétablissement prévu.

7.9. En cas de perturbation du service, les États membres, Eurojust et le Parquet européen assurent un recouvrement rapide des services et la perte minimale de données, conformément à la durée maximale d'interruption admissible et à la perte de données maximale admissible.

7.10. Les États membres, Eurojust et le Parquet européen mettent en œuvre les mesures appropriées pour atteindre les objectifs de disponibilité décrits ci-dessus et établissent des procédures pour réagir efficacement aux incidents.

8. **Autorités compétentes/base de données des cours et tribunaux (CDB)**

8.1. Conformément à l'article 19 du règlement (UE) 2023/1543, il est essentiel, aux fins du fonctionnement du système informatique décentralisé, de créer une source authentique sur les fournisseurs de services et les autorités compétentes.

8.2. La source authentique des autorités compétentes comporte les informations suivantes dans un format structuré:

a) aux fins de l'article 19 du règlement (UE) 2023/1543, des informations sur les autorités compétentes notifiées conformément à son article 31, paragraphe 1, points a) à c), y compris en ce qui concerne:

1) les membres nationaux d'Eurojust, assorties d'une indication précisant s'ils disposent d'une autorisation, au titre du droit national, d'émettre des injonctions européennes de production et de conservation en vertu de l'article 8, paragraphes 3 et 4, du règlement (UE) 2018/1727 du Parlement européen et du Conseil ([7]);

2) les procureurs européens délégués et les procureurs européens, lorsqu'ils sont notifiés par les États membres conformément à l'article 105, paragraphe 3, du règlement (UE) 2017/1939 du Conseil ([8]) en tant qu'autorité d'émission compétente au sens du règlement (UE) 2023/1543;

b) le cas échéant, des informations nécessaires pour déterminer les zones géographiques relevant de la compétence des autorités, ou d'autres critères pertinents nécessaires pour établir leur compétence;

c) des informations nécessaires au bon fonctionnement et à l'acheminement technique des messages des échanges de données au sein du système informatique décentralisé.

8.2.1. Les informations visées au point 8.2 c) comprennent les éléments suivants:

a) les informations sur l'État membre dans lequel est établi l'établissement désigné du fournisseur de services ou dans lequel réside son représentant légal:

1) État membre;

2) autorité centrale;

([7]) Règlement (UE) 2018/1727 du Parlement européen et du Conseil du 14 novembre 2018 relatif à l'Agence de l'Union européenne pour la coopération judiciaire en matière pénale (Eurojust) et remplaçant et abrogeant la décision 2002/187/JAI du Conseil (JO L 295 du 21.11.2018, p. 138).

([8]) Règlement (UE) 2017/1939 du Conseil du 12 octobre 2017 mettant en œuvre une coopération renforcée concernant la création du Parquet européen (JO L 283 du 31.10.2017, p. 1).

b) les informations sur le fournisseur de services:

1) nom;

2) adresse/siège;

3) numéro d'enregistrement;

4) forme juridique;

5) numéro de téléphone;

6) courriel;

c) les informations sur l'établissement désigné/le représentant légal:

1) type d'entité (établissement désigné/représentant légal);

2) nom;

3) adresse/siège;

4) numéro de téléphone;

5) courriel;

6) personne/entité de contact général;

7) langue(s) officielle(s) acceptée(s) par le fournisseur de services/l'établissement désigné/le représentant légal;

8) services visés à l'article 2, paragraphe 1, de la directive (UE) 2023/1544 du Parlement européen et du Conseil ([9]) proposés dans l'Union;

9) type d'instruments juridiques de l'Union pour lesquels l'établissement désigné/le représentant légal est désigné (dans les situations où les États membres ne participent pas à tous les instruments juridiques pertinents de l'Union);

10) champ d'application territorial de la désignation/nomination;

d) l'authentification des informations:

1) nom du représentant autorisé;

2) intitulé du poste;

3) adresse;

4) numéro de téléphone;

5) courriel;

6) date.

8.2.2. Lorsqu'elles sont disponibles, les informations visées au point 8.2 c) peuvent comprendre:

a) les informations sur le fournisseur de services:

1) personne de contact pour les questions concernant les notifications (si différente du signataire);

2) site web;

b) les types de données disponibles:

1) pour chaque service concerné:

— types de données disponibles,

— catégorie de données,

— identifiants,

— période de disponibilité des données;

([9]) Directive (UE) 2023/1544 du Parlement européen et du Conseil du 12 juillet 2023 établissant des règles harmonisées concernant la désignation d'établissements désignés et de représentants légaux aux fins de l'obtention de preuves électroniques dans le cadre des procédures pénales (JO L 191 du 28.7.2023, p. 181, ELI: http://data.europa.eu/eli/dir/2023/1544/oj).

2) informations complémentaires sur les données;

3) informations complémentaires sur le service (par exemple, relations de sous-traitance);

c) les informations sur l'établissement désigné/le représentant légal:

1) autres fournisseurs de services pour lesquels cet établissement désigné ou représentant légal est désigné;

2) coordonnées de l'assistance technique;

3) personne à contacter en cas d'urgence;

d) les informations techniques:

1) nom du point de contact technique;

2) numéro de téléphone du point de contact technique;

3) courriel du point de contact technique;

4) URL de l'API pour la récupération dynamique d'informations sur les types de données;

5) type de connexion au système informatique national:

— interface web,

— API,

— URL de l'API Push.

8.3. Compte tenu des besoins opérationnels du système informatique décentralisé:

a) la Commission est responsable du développement, de la maintenance, du fonctionnement et du soutien de la source authentique;

b) la Commission rend possible l'accès à la source authentique au moyen d'une API mise à la disposition des autorités compétentes, d'Eurojust et du Parquet européen aux fins de leur participation au système informatique décentralisé;

c) les États membres veillent à ce que les informations relatives à leurs autorités compétentes visées aux points 8.2 a) et b) de la source authentique soient complètes, exactes et tenues à jour;

d) la source authentique permet aux États membres de fournir et de mettre à jour les informations sur leurs fournisseurs de services y figurant, et elle permet aux autorités participant au système informatique décentralisé d'accéder à ces informations au moyen de programmes et de les récupérer;

e) les États membres et les fournisseurs de services veillent à ce que les informations visées au point 8.2 c) de la source authentique soient complètes, exactes et tenues à jour.