

**DÉCISION D'EXÉCUTION (UE) 2016/650 DE LA COMMISSION****du 25 avril 2016****établissant des normes relatives à l'évaluation de la sécurité des dispositifs qualifiés de création de signature électronique et de cachet électronique conformément à l'article 30, paragraphe 3, et à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014 du Parlement européen et du Conseil sur l'identification électronique et les services de confiance pour les transactions électroniques au sein du marché intérieur****(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) 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 <sup>(1)</sup>, et notamment son article 30, paragraphe 3, et son article 39, paragraphe 2,

considérant ce qui suit:

- (1) L'annexe II du règlement (UE) n° 910/2014 définit les exigences applicables aux dispositifs de création de signature électronique qualifiés et aux dispositifs de création de cachet électronique qualifiés.
- (2) La tâche d'élaborer des spécifications techniques nécessaires à la production et à la mise sur le marché de produits en tenant compte de l'état de la technologie est réalisée par des organismes compétents dans le domaine de la normalisation.
- (3) L'ISO/IEC (Organisation internationale de normalisation/Commission électrotechnique internationale) établit les concepts et principes généraux de la sécurité informatique et détermine le modèle général d'appréciation sur lequel doit reposer l'évaluation des propriétés des produits informatiques en matière de sécurité.
- (4) Dans le cadre du mandat de normalisation M/460 qui lui a été accordé par la Commission, le Comité européen de normalisation (CEN) a élaboré des normes applicables aux dispositifs de création de signature électronique et de cachet électronique qualifiés, lorsque les données de création de signature électronique ou de cachet électronique sont conservées dans un environnement dont l'utilisateur a la gestion totale, mais pas nécessairement exclusive. Ces normes sont jugées adaptées à l'évaluation de la conformité de ces dispositifs avec les exigences applicables énoncées à l'annexe II du règlement (UE) n° 910/2014.
- (5) Conformément à l'annexe II du règlement (UE) n° 910/2014, la gestion de données de création de signature électronique pour le compte d'un signataire peut être seulement confiée à un prestataire de services de confiance qualifié. Les exigences de sécurité et leurs spécifications de certification respectives sont différentes lorsque le signataire possède matériellement un produit et lorsqu'un prestataire de services de confiance qualifié exerce des activités pour le compte du signataire. Afin de traiter ces deux cas de figure et de favoriser, au fil du temps, le développement de produits et l'élaboration de normes d'évaluation adaptées à des besoins spécifiques, l'annexe de la présente décision devrait énumérer des normes relatives aux deux cas de figure.
- (6) Au moment de l'adoption de la présente décision de la Commission, plusieurs prestataires de services de confiance offrent déjà des solutions de gestion de données de création de signature électronique pour le compte de leurs clients. Les certifications de produits sont actuellement limitées aux modules matériels de sécurité certifiés conformes à différentes normes, mais pas encore spécifiquement certifiés conformes aux exigences applicables aux dispositifs de création de signature électronique et de cachet électronique qualifiés. Il n'existe toutefois pas encore de normes publiées, telles que la norme EN 419211 (applicable à la création de signature électronique dans un environnement dont l'utilisateur a la gestion totale, mais pas nécessairement exclusive), pour le marché tout aussi important des produits à distance certifiés. Les normes susceptibles d'être adaptées à cette fin étant actuellement en cours d'élaboration, la Commission complétera la présente décision lorsque ces normes seront disponibles et jugées conformes aux exigences prévues à l'annexe II du règlement (UE) n° 910/2014. Dans l'attente de l'établissement de la liste desdites normes, il est possible d'utiliser un autre processus pour évaluer la conformité de ces produits dans les conditions prévues à l'article 30, paragraphe 3, point b), du règlement (UE) n° 910/2014.
- (7) L'annexe de la présente décision mentionne la norme EN 419211, qui est composée de différentes parties (1 à 6) couvrant chacune un cas de figure différent. Les parties 5 et 6 de la norme EN 419211 fournissent des extensions

<sup>(1)</sup> JO L 257 du 28.8.2014, p. 73.

relatives à l'environnement pour des dispositifs de création de signature électronique qualifiés, comme la communication avec des applications de création de signature de confiance. Les fabricants de produits sont libres d'appliquer ces extensions. Conformément au considérant 56 du règlement (UE) n° 910/2014, la certification en vertu des articles 30 et 39 dudit règlement ne devrait pas s'étendre au-delà de la protection des données de création de signature électronique, et les applications de création de signature électronique ne sont pas couvertes par la certification.

- (8) Pour garantir que les signatures ou cachets électroniques générés au moyen d'un dispositif qualifié de création de signature électronique ou de cachet électronique sont protégés de manière fiable contre toute falsification, comme l'exige l'annexe II du règlement (UE) n° 910/2014, il est indispensable, pour la sécurité du produit certifié, de recourir à des algorithmes cryptographiques, des longueurs de clés et des fonctions de hachage appropriés. Cette question n'ayant pas été harmonisée au niveau européen, les États membres devraient coopérer afin de convenir des algorithmes cryptographiques, des longueurs de clés et des fonctions de hachage à utiliser dans le domaine des signatures et cachets électroniques.
- (9) L'adoption de la présente décision rend obsolète la décision 2003/511/CE de la Commission <sup>(1)</sup>. Il y a donc lieu de l'abroger.
- (10) Les mesures prévues à la présente décision sont conformes à l'avis du comité visé à l'article 48 du règlement (UE) n° 910/2014,

A ADOPTÉ LA PRÉSENTE DÉCISION:

#### *Article premier*

1. Les normes relatives à l'évaluation de la sécurité des produits informatiques qui s'appliquent à la certification des dispositifs qualifiés de création de signature électronique ou de création de cachet électronique conformément à l'article 30, paragraphe 3, point a), ou à l'article 39, paragraphe 2, du règlement (UE) n° 910/2014, lorsque les données de création de signature électronique ou les données de création de cachet électronique sont conservées dans un environnement dont l'utilisateur a la gestion totale, mais pas nécessairement exclusive, sont énumérées à l'annexe de la présente décision.

2. Dans l'attente de l'établissement par la Commission d'une liste de normes relatives à l'évaluation de la sécurité des produits informatiques qui s'appliquent à la certification des dispositifs qualifiés de création de signature électronique ou de création de cachet électronique, lorsqu'un prestataire de services de confiance qualifié gère les données de création de signature électronique ou de cachet électronique pour le compte d'un signataire ou d'un créateur de cachet, la certification de ces produits est fondée sur un processus qui, en vertu de l'article 30, paragraphe 3, point b), recourt à des niveaux de sécurité comparables à ceux requis par l'article 30, paragraphe 3, point a), et qui est notifié à la Commission par l'organisme public ou privé visé à l'article 30, paragraphe 1, du règlement (UE) n° 910/2014.

#### *Article 2*

La décision 2003/511/CE est abrogée.

#### *Article 3*

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 25 avril 2016.

Par la Commission  
Le président  
Jean-Claude JUNCKER

---

<sup>(1)</sup> Décision 2003/511/CE de la Commission du 14 juillet 2003 relative à la publication des numéros de référence de normes généralement admises pour les produits de signatures électroniques conformément à la directive 1999/93/CE du Parlement européen et du Conseil (JOL 175 du 15.7.2003, p. 45).

## ANNEXE

LISTE DES NORMES VISÉES À L'ARTICLE 1<sup>er</sup>, PARAGRAPHE 1

- ISO/IEC 15408 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Parties 1 à 3, telles qu'elles sont énumérées ci-dessous:
    - ISO/IEC 15408-1:2009 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 1. ISO, 2009,
    - ISO/IEC 15408-2:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 2. ISO, 2008,
    - ISO/IEC 15408-3:2008 — Technologies de l'information — Techniques de sécurité — Critères d'évaluation pour la sécurité TI — Partie 3. ISO, 2008;

et

  - ISO/IEC 18045:2008 — Technologies de l'information — Techniques de sécurité — Méthodologie pour l'évaluation de sécurité TI;

et

  - EN 419211 — Profils de protection pour dispositif sécurisé de création de signature électronique — Parties 1 à 6, selon le cas, telles qu'elles sont énumérées ci-dessous:
    - EN 419211-1:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 1: Présentation générale,
    - EN 419211-2:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 2: Dispositif avec génération de clé,
    - EN 419211-3:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 3: Dispositif avec import de clé,
    - EN 419211-4:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 4: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de génération de certificats,
    - EN 419211-5:2013 — Profils de protection des dispositifs sécurisés de création de signature — Partie 5: Extension pour un dispositif avec génération de clé et communication sécurisée avec l'application de création de signature,
    - EN 419211-6:2014 — Profils de protection pour dispositif sécurisé de création de signature électronique — Partie 6: Extension pour un dispositif avec import de clé et communication sécurisée avec l'application de création de signature.
-