Conseil de
l'Union européenne

Bruxelles, le 16 septembre 2022
(OR. en)

12429/22
ADD 1

Dossier interinstitutionnel:
2022/0272(COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

NOTE DE TRANSMISSION

Origine:	Pour la secrétaire générale de la Commission européenne, Madame Martine DEPREZ, directrice
Date de réception:	15 septembre 2022
Destinataire:	Secrétariat général du Conseil
N° doc. Cion:	COM(2022) 454 final - Annexes
Objet:	ANNEXES de la PROPOSITION DE RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

Les délégations trouveront ci-joint le document COM(2022) 454 final - Annexes.

p.j.: COM(2022) 454 final - Annexes

COMMISSION
EUROPÉENNE

Bruxelles, le 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

ANNEXES

de la

PROPOSITION DE RÈGLEMENT DU PARLEMENT EUROPÉEN ET DU CONSEIL

concernant des exigences horizontales en matière de cybersécurité pour les produits comportant des éléments numériques et modifiant le règlement (UE) 2019/1020

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

ANNEXE I

EXIGENCES ESSENTIELLES EN MATIÈRE DE CYBERSÉCURITÉ

1. EXIGENCES DE SECURITE RELATIVES AUX PROPRIETES DES PRODUITS COMPORTANT DES ELEMENTS NUMERIQUES

(1) Les produits comportant des éléments numériques sont conçus, développés et fabriqués de manière à garantir un niveau de cybersécurité approprié en fonction des risques.

(2) Les produits comportant des éléments numériques doivent être livrés sans aucune vulnérabilité exploitable connue.

(3) Sur la base de l'évaluation des risques visée à l'article 10, paragraphe 2, les produits comportant des éléments numériques doivent, le cas échéant:

(a) être livrés avec une configuration de sécurité par défaut, y compris la possibilité de réinitialiser le produit à son état d'origine;

(b) assurer la protection contre les accès non autorisés par des mécanismes de contrôle appropriés, y compris, mais sans s'y limiter, des systèmes d'authentification, d'identité ou de gestion des accès;

(c) protéger la confidentialité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, par exemple en chiffrant les données pertinentes au repos ou en transit au moyen de mécanismes de pointe;

(d) protéger l'intégrité des données stockées, transmises ou traitées de toute autre manière, à caractère personnel ou autres, des commandes, des programmes et de la configuration contre toute manipulation ou modification non autorisée par l'utilisateur, ainsi que signaler les corruptions;

(e) ne traiter que les données, à caractère personnel ou autres, qui sont adéquates, pertinentes et limitées à ce qui est nécessaire par rapport à l'utilisation prévue du produit («minimisation des données»);

(f) protéger la disponibilité des fonctions essentielles, y compris la résilience et l'atténuation des attaques par déni de service;

(g) réduire au maximum leurs propres effets négatifs sur la disponibilité des services fournis par d'autres dispositifs ou réseaux;

(h) être conçus, développés et fabriqués de manière à limiter les surfaces d'attaque, y compris les interfaces externes;

(i) être conçus, développés et fabriqués de manière à réduire les conséquences d'un incident, en utilisant des mécanismes et des techniques appropriés de limitation de l'exploitation de failles;

(j) fournir des informations relatives à la sécurité en enregistrant et/ou en surveillant les activités internes pertinentes, y compris l'accès ou la modification des données, des services ou des fonctions;

(k) garantir que les vulnérabilités puissent être traitées par des mises à jour de sécurité, y compris, le cas échéant, par des mises à jour automatiques et la notification des mises à jour disponibles aux utilisateurs.

2. EXIGENCES RELATIVES A LA GESTION DES VULNERABILITES

Les fabricants des produits comportant des éléments numériques doivent:

(1) recenser et documenter les vulnérabilités et les composants contenus dans le produit, notamment en établissant une nomenclature des logiciels dans un format couramment utilisé et lisible par machine couvrant au moins les dépendances de niveau supérieur du produit;

(2) s'agissant des risques posés aux produits comportant des éléments numériques, gérer et corriger sans délai les vulnérabilités, notamment en fournissant des mises à jour de sécurité;

(3) soumettre régulièrement les produits comportant des éléments numériques à des tests et examens de sécurité efficaces;

(4) dès la publication d'une mise à jour de sécurité, divulguer publiquement des informations sur les vulnérabilités corrigées, en ce compris une description des vulnérabilités, des informations permettant aux utilisateurs d'identifier le produit concerné, les conséquences de ces vulnérabilités, leur gravité et des informations aidant les utilisateurs à y remédier;

(5) mettre en place et appliquer une politique de divulgation coordonnée des vulnérabilités;

(6) prendre des mesures pour faciliter le partage d'informations sur les vulnérabilités potentielles de leurs produits comportant des éléments numériques ainsi que des composants tiers contenus dans ces produits, y compris en fournissant une adresse de contact pour le signalement des vulnérabilités découvertes dans les produits concernés;

(7) prévoir des mécanismes de distribution sécurisée des mises à jour pour les produits comportant des éléments numériques afin de s'assurer que les vulnérabilités exploitables soient corrigées ou atténuées rapidement;

(8) veiller à ce que, lorsque des correctifs ou des mises à jour de sécurité sont disponibles pour remédier à des problèmes de sécurité constatés, ils soient diffusés sans délai et gratuitement, et accompagnés de messages de recommandation fournissant aux utilisateurs les informations pertinentes, notamment sur les éventuelles mesures à prendre.

ANNEXE II

INFORMATIONS ET INSTRUCTIONS DESTINÉES À L'UTILISATEUR

Le produit comportant des éléments numériques doit au moins être accompagné des informations et instructions suivantes:

1. le nom, la raison sociale ou la marque déposée du fabricant, et les adresses postale et électronique auxquelles il peut être contacté, sur le produit ou, lorsque cela n'est pas possible, sur l'emballage ou dans un document accompagnant le produit;
2. le point de contact où les informations sur les vulnérabilités du produit en matière de cybersécurité peuvent être signalées et reçues;
3. l'identification correcte du type, du lot, de la version ou du numéro de série ou tout autre élément permettant l'identification du produit, ainsi que les instructions et informations d'utilisation correspondantes;
4. l'utilisation prévue, y compris l'environnement de sécurité fourni par le fabricant, ainsi que les fonctionnalités essentielles du produit et les informations sur ses propriétés de sécurité;
5. toutes circonstances connues ou prévisibles liées à l'utilisation du produit comportant des éléments numériques conformément à son utilisation prévue ou dans des conditions de mauvaise utilisation raisonnablement prévisible, susceptibles d'entraîner des risques de cybersécurité importants;
6. le cas échéant, l'endroit où la nomenclature des logiciels peut être consultée;
7. le cas échéant, l'adresse internet à laquelle la déclaration UE de conformité peut être consultée;
8. le type d'assistance technique en matière de sécurité proposé par le fabricant et la date de fin de celle-ci, à tout le moins la date jusqu'à laquelle les utilisateurs peuvent s'attendre à recevoir des mises à jour de sécurité;
9. des instructions détaillées ou une adresse internet renvoyant à des instructions détaillées et informations sur:
   (a) les mesures nécessaires lors de la mise en service initiale du produit et pendant toute sa durée de vie pour assurer sa sécurité d'utilisation,
   (b) la façon dont les modifications apportées au produit peuvent affecter la sécurité des données,
   (c) la façon dont les mises à jour pertinentes pour la sécurité peuvent être installées,
   (d) la mise hors service sécurisée du produit, en ce compris des informations sur la manière dont les données utilisateur peuvent être supprimées en toute sécurité.

ANNEXE III

PRODUITS CRITIQUES COMPORTANT DES ÉLÉMENTS NUMÉRIQUES

Classe I

1. logiciels de gestion des identités et logiciels de gestion des accès privilégiés;
2. navigateurs autonomes et intégrés;
3. gestionnaires de mots de passe;
4. logiciels qui recherchent, suppriment ou mettent en quarantaine des logiciels malveillants;
5. produits comportant des éléments numériques avec la fonction de réseau privé virtuel (VPN);
6. systèmes de gestion de la qualité;
7. outils de gestion des configurations de réseau;
8. systèmes de surveillance du trafic réseau;
9. gestion des ressources réseau;
10. systèmes de gestion des informations et des événements de sécurité (SIEM);
11. gestion des mises à jour/correctifs, y compris les gestionnaires de démarrage;
12. systèmes de gestion de la configuration des applications;
13. logiciels d'accès/de partage à distance;
14. logiciels de gestion des appareils mobiles;
15. interfaces réseau physiques;
16. systèmes d'exploitation non couverts par la classe II;
17. pare-feu, systèmes de détection et/ou de prévention des intrusions non couverts par la classe II;
18. routeurs, modems destinés à la connexion à l'internet et commutateurs, non couverts par la classe II;
19. microprocesseurs non couverts par la classe II;
20. microcontrôleurs;
21. circuits intégrés spécifiques aux applications et réseaux de portes programmables destinés à être utilisés par des entités essentielles du type visé à l'[annexe I de la directive XXX/XXXX (NIS2)];
22. systèmes d'automatisation et de contrôle industriels non couverts par la classe II, tels que les contrôleurs logiques programmables (PLC), les systèmes de contrôle distribués, les contrôleurs numériques informatisés pour machines-outils (CNC) et les systèmes de contrôle et d'acquisition de données (SCADA);
23. internet industriel des objets non couvert par la classe II.

Classe II

1. systèmes d’exploitation pour serveurs, ordinateurs de bureau et appareils mobiles;
2. hyperviseurs et systèmes d’exécution de conteneurs prenant en charge l’exécution virtualisée de systèmes d’exploitation et d’environnements similaires;
3. émetteurs de certificats numériques et d’infrastructure à clé publique;
4. pare-feu, systèmes de détection et/ou de prévention des intrusions destinés à un usage industriel;
5. microprocesseurs à usage général;
6. microprocesseurs destinés à être intégrés dans des contrôleurs logiques programmables et des éléments sécurisés;
7. routeurs, modems destinés à la connexion à l’internet et commutateurs, destinés à un usage industriel;
8. éléments sécurisés;
9. modules matériels de sécurité (HSM);
10. cryptoprocesseurs sécurisés;
11. cartes à puce, lecteurs de cartes à puce et jetons;
12. systèmes d’automatisation et de contrôle industriels destinés à être utilisés par des entités essentielles du type visé à l’[annexe I de la directive XXX/XXXX (NIS2)], telles que les contrôleurs logiques programmables (PLC), les systèmes de contrôle distribués, les contrôleurs numériques informatisés pour machines-outils (CNC) et les systèmes de contrôle et d’acquisition de données (SCADA);
13. dispositifs de l’internet des objets industriel destinés à être utilisés par des entités essentielles du type visé à l’[annexe I de la directive XXX/XXXX (NIS2)];
14. composants de détection et d’actionneur de robot et contrôleurs de robots;
15. compteurs intelligents.

ANNEXE IV

DÉCLARATION UE DE CONFORMITÉ

La déclaration UE de conformité prévue à l'article 20 contient l'ensemble des informations suivantes:

1. nom et type, ainsi que toute information supplémentaire permettant l'identification unique du produit comportant des éléments numériques;
2. nom et adresse du fabricant ou de son mandataire;
3. attestation certifiant que la déclaration UE de conformité est établie sous la seule responsabilité du fournisseur;
4. objet de la déclaration (identification du produit permettant sa traçabilité; au besoin, une photographie peut être jointe);
5. une mention indiquant que l'objet de la déclaration décrit ci-dessus est conforme à la législation d'harmonisation de l'Union applicable:
6. les références de toute norme harmonisée pertinente appliquée ou de toute autre spécification commune ou certification de cybersécurité par rapport auxquelles la conformité est déclarée;
7. le cas échéant, le nom et le numéro de l'organisme notifié, une description de la procédure d'évaluation de la conformité suivie et la référence du certificat délivré;
8. informations supplémentaires:

Signé par et au nom de: ……

(date et lieu d'établissement):

(nom, fonction) (signature):

ANNEXE V

CONTENU DE LA DOCUMENTATION TECHNIQUE

La documentation technique visée à l'article 23 contient au moins les informations ci-après, selon le produit comportant des éléments numériques concerné:

1. une description générale du produit comportant des éléments numériques, y compris:
   (a) l'utilisation prévue;
   (b) les versions de logiciel ayant des incidences sur la conformité aux exigences essentielles;
   (c) lorsque le produit comportant des éléments numériques est un produit matériel, des photographies ou des illustrations montrant les caractéristiques extérieures, le marquage et la disposition intérieure;
   (d) les informations et instructions destinées à l'utilisateur figurant à l'annexe II;
2. une description de la conception, du développement et de la fabrication du produit et des processus de gestion des vulnérabilités, et notamment:
   (a) des informations complètes sur la conception et le développement du produit comportant des éléments numériques, y compris, le cas échéant, des dessins et des schémas et/ou une description de l'architecture du système expliquant comment les composants logiciels s'appuient les uns sur les autres ou s'alimentent et s'intègrent dans le traitement global;
   (b) des informations et des spécifications complètes concernant le processus de gestion des vulnérabilités mis en place par le fabricant, en ce compris la nomenclature des logiciels, la politique coordonnée de divulgation des vulnérabilités, la preuve de la fourniture d'une adresse de contact pour le signalement des vulnérabilités et une description des solutions techniques choisies pour la distribution sécurisée des mises à jour;
   (c) des informations et des spécifications complètes concernant les processus de production et de suivi du produit comportant des éléments numériques et la validation de ces processus;
3. une évaluation des risques de cybersécurité sur la base de laquelle le produit comportant des éléments numériques est conçu, développé, produit, livré et entretenu, conformément à l'article 10 du présent règlement;
4. une liste des normes harmonisées, appliquées entièrement ou en partie, dont les références ont été publiées au *Journal officiel de l'Union européenne*, des spécifications communes telles que définies à l'article 19 du présent règlement ou des schémas de certification de cybersécurité au titre du règlement (UE) 2019/881, conformément à l'article 18, paragraphe 3, et, lorsque ces normes harmonisées, spécifications communes ou schémas de certification de cybersécurité n'ont pas été appliqués, une présentation des solutions adoptées pour répondre aux exigences essentielles exposées à l'annexe I, sections 1 et 2, y compris une liste des autres spécifications techniques pertinentes appliquées. Dans le cas où des normes harmonisées, spécifications communes ou certifications de cybersécurité ont été appliquées en partie, la documentation technique précise les parties appliquées;

5. les rapports des essais effectués pour vérifier la conformité du produit et des processus de gestion des vulnérabilités aux exigences essentielles applicables énoncées à l'annexe I, sections 1 et 2;

6. une copie de la déclaration UE de conformité;

7. le cas échéant, la nomenclature des logiciels telle que définie à l'article 3, point 36, à la suite d'une demande motivée d'une autorité de surveillance du marché, pour autant que celle-ci soit nécessaire pour permettre à cette autorité de vérifier le bon respect des exigences essentielles énoncées à l'annexe I.

ANNEXE VI

PROCÉDURES D'ÉVALUATION DE LA CONFORMITÉ

Procédure d'évaluation de la conformité basée sur le contrôle interne (basée sur le module A)

1. Le contrôle interne correspond à la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations énoncées aux points 2, 3 et 4, assure et déclare sous sa seule responsabilité que les produits comportant des éléments numériques satisfont à toutes les exigences essentielles énoncées à l'annexe I, section 1, et par laquelle le fabricant satisfait aux exigences essentielles énoncées à l'annexe I, section 2.

2. Le fabricant établit la documentation technique décrite à l'annexe V.

3. Conception, développement, production et gestion des vulnérabilités des produits comportant des éléments numériques

   Le fabricant prend toutes les mesures nécessaires pour que les processus de conception, de développement, de production et de gestion des vulnérabilités ainsi que leur suivi garantissent la conformité des produits comportant des éléments numériques fabriqués ou développés et des processus mis en place par lui avec les exigences essentielles énoncées à l'annexe I, sections 1 et 2.

4. Marquage de conformité et déclaration de conformité

4.1. Le fabricant appose le marquage CE sur chaque produit comportant des éléments numériques qui répond aux exigences applicables du présent règlement.

4.2. Le fabricant établit une déclaration UE de conformité écrite pour chaque produit comportant des éléments numériques conformément à l'article 20 et la tient, accompagnée de la documentation technique, à la disposition des autorités nationales pendant dix ans à partir du moment où le produit concerné a été mis sur le marché. La déclaration UE de conformité précise le produit comportant des éléments numériques pour lequel elle a été établie. Une copie de la déclaration UE de conformité est mise à la disposition des autorités compétentes sur demande.

5. Mandataires

   Les obligations du fabricant énoncées au point 4 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant qu'elles soient spécifiées dans le mandat.

Examen UE de type (basé sur le module B)

1. L'examen UE de type correspond à la partie d'une procédure d'évaluation de la conformité dans laquelle un organisme notifié examine la conception technique et le développement d'un produit et les processus de gestion des vulnérabilités mis en place par le fabricant, et atteste qu'un produit comportant des éléments numériques satisfait aux exigences essentielles énoncées à l'annexe I, section 1, et que le fabricant satisfait aux exigences essentielles énoncées à l'annexe I, section 2.

– L’examen UE de type consiste en une évaluation de l’adéquation de la conception technique et du développement du produit par un examen de la documentation technique et des preuves visées au point 3, avec examen d’échantillons d’une ou de plusieurs parties critiques du produit (combinaison du type de fabrication et du type de conception).

2. Le fabricant introduit une demande d’examen UE de type auprès d’un seul organisme notifié de son choix.

Cette demande comporte:

– le nom et l’adresse du fabricant, ainsi que le nom et l’adresse du mandataire si la demande est introduite par celui-ci;

– une déclaration écrite certifiant que la même demande n’a pas été introduite auprès d’un autre organisme notifié;

– la documentation technique, qui permet d’évaluer la conformité du produit aux exigences essentielles applicables énoncées à l’annexe I, section 1, et les processus de gestion des vulnérabilités du fabricant énoncés à l’annexe I, section 2, et comprend une analyse et une évaluation adéquates du ou des risques. La documentation technique précise les exigences applicables et couvre, dans la mesure nécessaire à l’évaluation, la conception, la fabrication et le fonctionnement du produit. La documentation technique contient, le cas échéant, au moins les éléments énoncés à l’annexe V;

– les preuves à l’appui de l’adéquation des solutions de conception technique et de développement et des processus de gestion des vulnérabilités. Ces preuves mentionnent tous les documents qui ont été utilisés, en particulier lorsque les normes harmonisées et/ou les spécifications techniques applicables n’ont pas été appliquées dans leur intégralité. Elles comprennent, si nécessaire, les résultats des essais effectués par le laboratoire approprié du fabricant ou par un autre laboratoire d’essai en son nom et sous sa responsabilité.

3. L’organisme notifié:

3.1. examine la documentation technique et les éléments de preuve pour évaluer l’adéquation de la conception technique et du développement du produit aux exigences essentielles énoncées à l’annexe I, section 1, et des processus de gestion des vulnérabilités mis en place par le fabricant aux exigences essentielles énoncées à l’annexe I, section 2;

3.2. vérifie que le ou les échantillons ont été développés ou fabriqués en conformité avec la documentation technique et relève les éléments qui ont été conçus et développés conformément aux dispositions applicables des normes harmonisées et/ou des spécifications techniques pertinentes, ainsi que les éléments dont la conception et le développement ne s’appuient pas sur les dispositions pertinentes desdites normes;

3.3. effectue ou fait effectuer les examens et les essais appropriés pour vérifier si, dans le cas où le fabricant a choisi d’appliquer les solutions indiquées dans les normes harmonisées et/ou les spécifications techniques pertinentes pour les exigences énoncées à l’annexe I, celles-ci ont été appliquées correctement;

3.4. effectue ou fait effectuer les contrôles et les essais appropriés pour vérifier si, dans le cas où les solutions indiquées dans les normes harmonisées et/ou les spécifications techniques pertinentes pour les exigences de l’annexe I n’ont pas été appliquées, les

solutions adoptées par le fabricant satisfont aux exigences essentielles correspondantes;

3.5. convient avec le fabricant de l'endroit où les examens et les essais seront effectués.

4. L'organisme notifié établit un rapport d'évaluation répertoriant les activités effectuées conformément au point 4 et leurs résultats. Sans préjudice de ses obligations vis-à-vis des autorités notifiantes, l'organisme notifié ne divulgue le contenu de ce rapport, en totalité ou en partie, qu'avec l'accord du fabricant.

5. Lorsque le type et les processus de gestion des vulnérabilités satisfont aux exigences essentielles énoncées à l'annexe I, l'organisme notifié délivre au fabricant une attestation d'examen UE de type. L'attestation contient le nom et l'adresse du fabricant, les conclusions de l'examen, les conditions (éventuelles) de sa validité et les données nécessaires à l'identification du type et des processus de gestion des vulnérabilités approuvés. Une ou plusieurs annexes peuvent être jointes à l'attestation.

L'attestation et ses annexes contiennent toutes les informations nécessaires pour permettre l'évaluation de la conformité des produits fabriqués ou développés au type examiné et des processus de gestion des vulnérabilités à évaluer et pour permettre un contrôle en service.

Lorsque le type et les processus de gestion des vulnérabilités ne satisfont pas aux exigences essentielles applicables énoncées à l'annexe I, l'organisme notifié refuse de délivrer une attestation d'examen UE de type et en informe le demandeur, en lui précisant les raisons de son refus.

6. L'organisme notifié suit l'évolution de l'état de la technique généralement reconnu, et lorsque cette évolution donne à penser que le type et les processus de gestion des vulnérabilités approuvés pourraient ne plus être conformes aux exigences essentielles applicables énoncées à l'annexe I, il détermine si des examens complémentaires sont nécessaires. Si tel est le cas, l'organisme notifié en informe le fabricant.

Le fabricant informe l'organisme notifié qui détient la documentation technique relative à l'attestation d'examen UE de type de toutes les modifications du type et des processus de gestion des vulnérabilités approuvés qui peuvent remettre en cause la conformité aux exigences essentielles énoncées à l'annexe I, ou les conditions de validité de l'attestation. Ces modifications nécessitent une nouvelle approbation sous la forme d'un complément à l'attestation initiale d'examen UE de type.

7. Chaque organisme notifié informe ses autorités notifiantes des attestations d'examen UE de type et/ou des compléments qu'il a délivrés ou retirés et leur transmet, périodiquement ou sur demande, la liste des attestations et/ou des compléments qu'il a refusés, suspendus ou soumis à d'autres restrictions.

Chaque organisme notifié informe les autres organismes notifiés des attestations d'examen UE de type et/ou des compléments qu'il a refusés, retirés, suspendus ou soumis à d'autres restrictions et, sur demande, des attestations et/ou des compléments qu'il a délivrés.

La Commission, les États membres et les autres organismes notifiés peuvent, sur demande, obtenir une copie des attestations d'examen UE de type et/ou de leurs compléments. Sur demande, la Commission et les États membres peuvent obtenir une copie de la documentation technique et des résultats des examens réalisés par l'organisme notifié. L'organisme notifié conserve une copie de l'attestation

d'examen UE de type, de ses annexes et compléments, ainsi que le dossier technique, y compris la documentation communiquée par le fabricant, jusqu'à la fin de la validité de ladite attestation.

8. Le fabricant tient à la disposition des autorités nationales une copie de l'attestation d'examen UE de type, de ses annexes et compléments, ainsi que la documentation technique, pour une durée de dix ans à partir du moment où le produit a été mis sur le marché.

9. Le mandataire du fabricant peut introduire la demande visée au point 3 et s'acquitter des obligations énoncées aux points 7 et 9 pour autant qu'elles soient spécifiées dans le mandat.

Conformité au type sur la base du contrôle interne de la fabrication (basée sur le module C)

1. La conformité au type sur la base du contrôle interne de la fabrication correspond à la partie de la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations définies aux points 2 et 3, et garantit et déclare que les produits concernés sont conformes au type décrit dans l'attestation d'examen UE de type et satisfont aux exigences essentielles énoncées à l'annexe I, section 1.

2. Production

2.1. Le fabricant prend toutes les mesures nécessaires pour que la production et le suivi de celle-ci garantissent la conformité des produits fabriqués au type approuvé décrit dans l'attestation d'examen UE de type et aux exigences essentielles énoncées à l'annexe I, section 1.

3. Marquage de conformité et déclaration de conformité

3.1. Le fabricant appose le marquage CE sur chaque produit conforme au type décrit dans l'attestation d'examen UE de type et satisfait aux exigences applicables de l'instrument législatif.

3.2. Le fabricant établit une déclaration écrite de conformité concernant un modèle de produit et la tient à la disposition des autorités nationales pendant une durée de dix ans à partir du moment où le produit a été mis sur le marché. La déclaration de conformité précise le modèle de produit pour lequel elle a été établie. Une copie de la déclaration de conformité est mise à la disposition des autorités compétentes sur demande.

4. Mandataire

Les obligations du fabricant visées au point 3 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, pour autant qu'elles soient spécifiées dans le mandat.

Conformité sur la base de l'assurance complète de la qualité (basée sur le module H)

1. La conformité sur la base de l'assurance complète de la qualité correspond à la procédure d'évaluation de la conformité par laquelle le fabricant remplit les obligations énoncées aux points 2 et 5, et garantit et déclare sous sa seule responsabilité que les produits (ou catégories de produits) concernés satisfont aux exigences essentielles énoncées à l'annexe I, section 1, et que les processus de

gestion des vulnérabilités mis en place par le fabricant satisfont aux exigences énoncées à l'annexe I, section 2.

2. Conception, développement, production et gestion des vulnérabilités des produits comportant des éléments numériques

Le fabricant applique un système de qualité approuvé, tel que spécifié au point 3, pour la conception, le développement et la fabrication des produits concernés et pour la gestion des vulnérabilités, maintient son efficacité tout au long du cycle de vie des produits concernés et fait l'objet d'une surveillance, tel que spécifié au point 4.

3. Système de qualité

3.1. Le fabricant introduit, auprès d'un organisme notifié de son choix, une demande d'évaluation de son système de qualité pour les produits concernés.

Cette demande comporte:

– le nom et l'adresse du fabricant, ainsi que le nom et l'adresse du mandataire si la demande est introduite par celui-ci;

– la documentation technique, pour un modèle de chaque catégorie de produits destinés à être fabriqués ou développés. La documentation technique contient, le cas échéant, au minimum les éléments énoncés à l'annexe V;

– la documentation relative au système de qualité; et

– une déclaration écrite certifiant que la même demande n'a pas été introduite auprès d'un autre organisme notifié.

3.2. Le système de qualité garantit la conformité des produits avec les exigences essentielles énoncées à l'annexe I, section 1, et la conformité des processus de gestion des vulnérabilités mis en place par le fabricant avec les exigences énoncées à l'annexe I, section 2.

Tous les éléments, exigences et dispositions adoptés par le fabricant sont réunis de manière systématique et ordonnée dans une documentation sous la forme de mesures, de procédures et d'instructions écrites. Cette documentation relative au système de qualité facilite une interprétation homogène des programmes, des plans, des manuels et des dossiers concernant la qualité.

Elle contient en particulier une description adéquate des éléments suivants:

– les objectifs de qualité, l'organigramme ainsi que les responsabilités et les compétences du personnel d'encadrement en matière de qualité de la conception, du développement et des produits, ainsi que de gestion des vulnérabilités;

– les spécifications de la conception technique et du développement, y compris les normes, qui seront appliquées et, lorsque les normes harmonisées et/ou les spécifications techniques pertinentes ne sont pas appliquées intégralement, les moyens qui seront utilisés pour faire en sorte de respecter les exigences essentielles énoncées à l'annexe I, section 1, qui s'appliquent aux produits;

– les spécifications des procédures, y compris les normes, qui seront appliquées et, lorsque les normes harmonisées et/ou les spécifications techniques pertinentes ne sont pas appliquées intégralement, les moyens qui

seront utilisés pour faire en sorte de respecter les exigences essentielles énoncées à l'annexe I, section 2, qui s'appliquent au fabricant;

– le contrôle de la conception et du développement, ainsi que les techniques de vérification de la conception et du développement, les procédés et les actions systématiques qui seront utilisés lors de la conception et du développement des produits appartenant à la catégorie couverte;

– les techniques correspondantes de production, de contrôle de la qualité et d'assurance de la qualité, les procédés et les actions systématiques qui seront utilisés;

– les examens et les essais qui seront effectués avant, pendant et après la production et la fréquence à laquelle ils auront lieu;

– les dossiers de qualité, tels que les rapports d'inspection et les données d'essais et d'étalonnage, les rapports sur la qualification du personnel concerné, etc.;

– les moyens de surveillance permettant de contrôler l'obtention de la qualité requise en matière de conception et de produit et le bon fonctionnement du système de qualité.

3.3. L'organisme notifié évalue le système de qualité pour déterminer s'il répond aux exigences visées au point 3.2.

Il présume la conformité à ces exigences pour les éléments du système de qualité qui sont conformes aux spécifications correspondantes de la norme nationale transposant la norme harmonisée applicable et/ou la spécification technique.

L'équipe d'auditeurs doit posséder une expérience des systèmes de gestion de la qualité et comporter au moins un membre ayant de l'expérience en tant qu'évaluateur dans le groupe de produits et la technologie concernés, ainsi qu'une connaissance des exigences applicables du présent règlement. L'audit comprend une visite d'évaluation dans les installations du fabricant, si de telles installations existent. L'équipe d'auditeurs examine la documentation technique visée au point 3.1, deuxième tiret, afin de vérifier la capacité du fabricant à déterminer les exigences applicables du présent règlement et à réaliser les examens nécessaires en vue de garantir la conformité du produit à ces exigences.

La décision est notifiée au fabricant ou à son mandataire.

La notification contient les conclusions de l'audit et la décision d'évaluation motivée.

3.4. Le fabricant s'engage à remplir les obligations découlant du système de qualité tel qu'il est approuvé et à faire en sorte qu'il demeure adéquat et efficace.

3.5. Le fabricant informe l'organisme notifié ayant approuvé le système de qualité de tout projet de modification de celui-ci.

L'organisme notifié examine les modifications envisagées et décide si le système de qualité modifié continuera de répondre aux exigences énoncées au point 3.2 ou si une nouvelle évaluation s'impose.

Il notifie sa décision au fabricant. La notification contient les conclusions de l'examen et la décision d'évaluation motivée.

4. Surveillance sous la responsabilité de l'organisme notifié

4.1. Le but de la surveillance est de s'assurer que le fabricant remplit correctement les obligations découlant du système de qualité approuvé.

4.2. Le fabricant autorise l'organisme notifié à accéder, à des fins d'évaluation, aux lieux de conception, de développement, de production, d'inspection, d'essai et de stockage et lui fournit toutes les informations nécessaires, notamment:

– la documentation sur le système de qualité;

– les dossiers de qualité prévus dans la partie du système de qualité consacrée à la conception, tels que les résultats des analyses, des calculs, des essais, etc.;

– les dossiers de qualité prévus par la partie du système de qualité consacrée à la fabrication, tels que les rapports d'inspection, les données d'essais et d'étalonnage, les rapports sur la qualification du personnel concerné, etc.

4.3. L'organisme notifié effectue périodiquement des audits pour s'assurer que le fabricant maintient et applique le système de qualité, et il transmet un rapport d'audit au fabricant.

5. Marquage de conformité et déclaration de conformité

5.1. Sur chaque produit qui satisfait aux exigences énoncées à l'annexe I, section 1, du présent règlement, le fabricant doit apposer le marquage CE et, sous la responsabilité de l'organisme notifié visé au point 3.1, le numéro d'identification de ce dernier.

5.2. Le fabricant établit une déclaration écrite de conformité concernant chaque modèle de produit et la tient à la disposition des autorités nationales pendant une durée de dix ans à partir du moment où le produit a été placé sur le marché. La déclaration de conformité précise le modèle de produit pour lequel elle a été établie.

Une copie de la déclaration de conformité est mise à la disposition des autorités compétentes sur demande.

6. Pendant une période d'au moins dix ans à compter de la mise sur le marché du produit, le fabricant doit tenir à la disposition des autorités nationales:

– la documentation technique visée au point 3.1;

– la documentation concernant le système de qualité visée au point 3.1;

– les modifications approuvées visées au point 3.5;

– les décisions et rapports de l'organisme notifié visés aux points 3.5, 4.3 et 4.4.

7. Chaque organisme notifié informe ses autorités notifiantes des approbations de systèmes de qualité délivrées ou retirées et leur transmet, périodiquement ou sur demande, la liste des approbations qu'il a refusées, suspendues ou soumises à d'autres restrictions.

Chaque organisme notifié informe les autres organismes notifiés des approbations de systèmes de qualité qu'il a refusées, suspendues ou retirées et, sur demande, des approbations qu'il a délivrées.

8. Mandataire

Les obligations du fabricant établies aux points 3.1, 3.5, 5 et 6 peuvent être remplies par son mandataire, en son nom et sous sa responsabilité, à condition qu'elles soient spécifiées dans le mandat.