Décret

Nº …/2024 (… …) du président de l'autorité de surveillance des affaires réglementaires (SZTFH)

relatif au système national de certification de la cybersécurité pour les dispositifs IdO

Sur la base de l'autorisation accordée à l'article 28, paragraphe 3, point *c)* de la loi XXIII de 2023 sur la certification de la cybersécurité et la surveillance de la cybersécurité et agissant dans le cadre de mes fonctions telles que définies à l'article 13, points *n)* et *q)* de la loi XXXII de 2021 relative à l'autorité de surveillance des affaires réglementaires, j'ordonne par la présente ce qui suit:

Article premier

(1) Aux fins du présent décret, on entend par «dispositif IdO». un produit TIC au sens de la loi XXIII de 2023 sur la certification de la cybersécurité et la surveillance de la cybersécurité (ci-après dénommée: «loi sur la certification de la cybersécurité»), qui interagit avec l'environnement par la transformation du signal. La forme d'interaction peut être:
a) la détection par laquelle le dispositif IdO collecte des données sur l'environnement, ou
b) une intervention qui déclenche des changements dans l'environnement.

(2) L'interaction avec l'environnement visée au paragraphe 1 peut se faire par:
a) une interface de programmation d'application (ci-après dénommée: «API».) qui permet à d'autres dispositifs informatiques de communiquer avec un dispositif IdO via l'application fournie par celui-ci;
b) une interface utilisateur qui permet une communication directe entre le dispositif IdO et l'utilisateur, ou
c) une connexion réseau qui assure la communication du dispositif IdO avec un réseau de communications électroniques dans le but de communiquer des données vers ou à partir d'un dispositif IdO, ou qui garantit l'accès à l'interface utilisateur du réseau.

(3) Aux fins de l'application du paragraphe 2, point *c)*, la capacité d'interface pour activer une connexion réseau comprend à la fois le matériel et l'environnement logiciel qui l'exploite et le sert.

Article 2

(1) Le présent décret, à l'exception des paragraphes 2 et 3, s'applique à l'autoévaluation et à l'évaluation de la conformité des dispositifs IdO (ci-après collectivement dénommées: «évaluation»).

(2) Le décret ne couvre pas l'évaluation des outils IdO pour lesquels un système national de certification de la cybersécurité a été établi dans un décret distinct, par le président de l'autorité de surveillance des affaires réglementaires (SZTFH).

(3) Le système national de certification de la cybersécurité pour les dispositifs IdO (ci-après dénommé: «système de certification») vise à garantir que les décisions prises par les citoyens, les organisations professionnelles et les organismes publics lors de l'acquisition de produits IdO sont soutenues et que les actifs sont comparables sur la base des niveaux d'assurance définis dans le système de certification.

Article 3

(1) Le système de certification contient des exigences relatives aux niveaux d'assurance «basique», «significatif» et «élevé» au sens de l'article 8, paragraphe 1, de la loi sur la certification de la cybersécurité.

(2) Sur la base du système de certification, l'autoévaluation de la conformité peut être effectuée au niveau d'assurance «basique».

(3) Les évaluations de la conformité par les organismes d'évaluation de la conformité peuvent être effectuées, tout au plus, au niveau d'assurance enregistré par l'autorité de surveillance des affaires réglementaires en tant qu'autorité nationale de certification de la cybersécurité désignée à l'article 4, paragraphe 1, point a), de la loi sur la certification de la cybersécurité (ci-après dénommée: «autorité de certification»), à la demande du fabricant, conformément à la loi sur la certification de la cybersécurité (ci-après dénommé: «fabricant»).

Article 4

(1) Un fabricant peut engager une procédure nationale d'autoévaluation de la conformité, ou un organisme d'évaluation de la conformité peut commencer les activités d'évaluation de la conformité, si les documents visés à l'annexe 1 et produits par le fabricant sont disponibles. Un modèle des documents visés à l'annexe 1 est publié sur le site internet de l'autorité de certification.

(2) La déclaration nationale de conformité ou le certificat national de cybersécurité (ensemble: «certificat national») ne peut être délivré pour le niveau d'assurance donné que si le dispositif IdO soumis à évaluation satisfait aux exigences énoncées à l'annexe 2 pour ledit niveau d'assurance.

(3) La conformité en vertu du paragraphe 2 peut être démontrée en présentant le rapport d'évaluation qui doit être délivré sur la base d'un examen effectué conformément à la méthode d'évaluation décrite à l'annexe 4 (ci-après dénommé: «rapport d'évaluation»), ou en effectuant un test de vulnérabilité pour les exigences énoncées à l'annexe 3.

(4) Les certificats délivrés sur la base d'une norme internationale, européenne ou nationale ne sont pas acceptés pour démontrer la conformité en vertu du paragraphe 2, au lieu des informations requises conformément au paragraphe 3.

(5) Un fabricant peut délivrer une déclaration de conformité en vertu de l'annexe 5 et un organisme d'évaluation de la conformité peut délivrer un certificat national de cybersécurité conformément à l'annexe 6 si le rapport d'évaluation apporte collectivement des résultats positifs avec une qualification «réussi».

(6) Le fabricant ou l'organisme d'évaluation de la conformité soumet le certificat national, les documents visés à l'annexe 1 et le rapport d'évaluation pour enregistrement à l'autorité de certification, au moyen d'un formulaire électronique établi à cet effet par l'autorité de certification.

(7) Le délai administratif d'enregistrement prévu au paragraphe 6 est de 45 jours.

Article 5

(1) La durée de validité du certificat national (ci-après dénommée: «durée de validité») est de 365 jours maximum à compter de la date d'émission.

(2) Le fabricant appose l'étiquette, visée à l'annexe 7, en tant que marquage de conformité sur un dispositif IdO qui dispose d'un certificat national produit jusqu'à la fin de la durée de validité et l'étiquette présente le contenu indiqué dans la décision de l'autorité de certification.

(3) Pendant la durée de validité, le fabricant effectue continuellement et consécutivement des analyses d'impact sur la sécurité pour chaque modification affectant un dispositif IdO, en indiquant:

a) la date de la modification;
b) le motif de la modification;
c) si la modification affecte les dispositifs IdO fabriqués avant cette dernière;
d) une description détaillée des éléments de la modification;
e) quels risques sont affectés par la modification et
f) si la modification répond à une vulnérabilité ou introduit un nouveau contrôle de sécurité.

(4) Aux fins du paragraphe 3, toute modification affectant le statut de sécurité du dispositif IdO, y compris l'apparition de nouvelles menaces et vulnérabilités, est considérée comme une modification.

(5) Le fabricant met à jour le document de mise en œuvre mentionné à l'annexe 1 de façon continue et consécutive pendant la durée de validité.

Article 6

(1) Le fabricant peut, à l'exception du paragraphe 5, présenter une demande de prorogation de la validité de la déclaration nationale de conformité dans le registre de l'autorité de certification (ci-après dénommée: «une demande de prorogation»), qui est présentée à l'autorité de certification au moyen d'un formulaire électronique créé à cet effet par l'autorité de certification, au plus tôt 60 jours avant l'expiration de la durée de validité, mais au plus tard 30 jours avant l'expiration de celle-ci.

(2) La demande de prorogation est accompagnée de l'analyse d'impact sur la sécurité visée à l'article 5, paragraphe 3, du document de mise en œuvre (visé à l'annexe 1) dans sa version mise à jour conformément à l'article 5, paragraphe 3 et de la nouvelle durée de validité demandée, qui n'excède pas 365 jours.

(3) Au cours de la procédure de prorogation, le délai administratif de l'autorité de certification est de 30 jours.

(4) L'autorité de certification peut fixer une durée de validité différente de la durée de validité indiquée dans la demande de prorogation, mais celle-ci devrait être d'au moins 120 jours, calculée à compter de la fin de la durée de validité initiale, s'il ne peut être établi qu'avec les modifications apportées au dispositif IdO examiné, ledit dispositif IdO satisfait en permanence aux exigences du système de certification et assure la réalisation des objectifs de sécurité à partir de la date de délivrance de la déclaration nationale de conformité. Si la nouvelle durée de validité indiquée dans la demande de prorogation est inférieure à 120 jours, l'autorité de certification établit la nouvelle durée de validité conformément à la demande.

(5) Dans le cas visé au paragraphe 4, le fabricant ne peut pas présenter une autre demande de prorogation pour la déclaration de conformité qui a été émise pour le dispositif IdO donné.

(6) Dans le cas visé au paragraphe 4, ou lorsque la durée de validité de la déclaration de conformité délivrée pour le dispositif IdO a expiré, le fabricant peut soumettre à l'autorité de certification une demande de renouvellement de la déclaration nationale de conformité du dispositif IdO, au moyen d'un formulaire électronique créé à cet effet par l'autorité de certification.

(7) La demande visée au paragraphe 6 est accompagnée de la nouvelle déclaration de conformité qui a été délivrée conformément à l'article 4, paragraphe 5, sur la base de l'examen visé à l'article 4, paragraphes 1 à 4, des documents visés à l'annexe 1 et du rapport d'évaluation.

(8) Le délai administratif pour la procédure de renouvellement visée au paragraphe 6 est de 45 jours.

(9) Les paragraphes 1 à 4 s'appliquent à la prorogation de la validité d'une nouvelle déclaration de conformité, qui a été enregistrée par l'autorité de certification sur la base d'une demande en vertu du paragraphe 6.

Article 7

(1) Afin de prolonger la durée de validité du certificat pour un dispositif IdO donné qui a été enregistré sur la base d'un certificat national de cybersécurité délivré par un organisme d'évaluation de la conformité, le fabricant met à la disposition de l'organisme d'évaluation de la conformité, dans les 60 jours précédant l'expiration de la durée de validité, les éléments suivants: l'analyse d'impact sur la sécurité visée à l'article 5, paragraphe 3 et le document de mise en œuvre (visé à l'annexe 1) dans sa version mise à jour conformément à l'article 5, paragraphe 5.

(2) Sur la base de l'examen des documents visés au paragraphe 1, pour autant que, même avec les modifications apportées au dispositif IdO en cours d'examen, le dispositif IdO respecte en permanence les exigences du système de certification et assure la réalisation des objectifs de sécurité à compter de la délivrance du certificat national de cybersécurité, il proroge le certificat expirant au plus tard huit jours avant l'expiration de la durée de validité, la nouvelle durée de validité n'excédant pas 365 jours à compter de la fin de la durée de validité initiale.

(3) Si, sur la base des documents visés au paragraphe 1, il ne peut être établi que le dispositif IdO examiné satisfait continuellement aux exigences du système de certification à compter de

la date de délivrance du certificat national de cybersécurité et qu'il garantit la réalisation des objectifs de sécurité, l'organisme d'évaluation de la conformité peut proroger le certificat expirant à condition que la nouvelle durée de validité ne dépasse pas 90 jours civils à compter de la fin de la durée de validité initiale.

(4) Dans le cas visé au paragraphe 3, la durée de validité du certificat national de cybersécurité délivré pour un dispositif IdO donné ne peut pas être prolongée après l'expiration de la nouvelle durée de validité visée au paragraphe 3. En revanche, son renouvellement peut être initié.

(5) Le fabricant peut initier le renouvellement du certificat national de cybersécurité du dispositif IdO auprès de l'organisme d'évaluation de la conformité dans le cas visé au paragraphe 3, ou lorsque la durée de validité du certificat national de cybersécurité a expiré.

(6) Dans le cadre du renouvellement, l'organisme d'évaluation de la conformité soumettra aux fins de l'enregistrement, au moyen d'un formulaire électronique créé à cet effet par l'autorité de certification, les éléments suivants: le nouveau certificat national de cybersécurité délivré conformément à l'article 4, paragraphe 5, sur la base de l'examen visé à l'article 4, paragraphes 1 à 4, ainsi que les documents visés à l'annexe 1 et le rapport d'évaluation.

Article 8

La durée de validité du certificat national ne sera pas affectée si, au cours de celle-ci, un nouveau système national de certification de la cybersécurité est établi pour le dispositif IdO conformément à l'article 2, paragraphe 2, mais par la suite, la durée de validité du certificat national pour le dispositif IdO ne peut pas être prolongée. Une demande de prorogation ne peut pas être introduite et le certificat national ne peut pas être renouvelé.

Article 9

Le présent décret entre en vigueur le troisième jour suivant celui de sa publication.

Article 10

L'exigence de notification préalable du présent projet de décret, comme le prévoient les articles 5 à 7 de la directive (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information, est remplie.

Exigences relatives à la documentation

1. **Document d'identification des dispositifs IdO**

1.1. Le document contenant des informations permettant d'identifier le dispositif IdO faisant l'objet d'une autoévaluation de la conformité ou d'une évaluation de la conformité (ci-après dénommée: «VE»), qui contient des informations aussi détaillées que possible sur le sujet de l'examen, notamment en termes de numéros de versions et d'options de configuration.

1.2. Contenu minimal du document d'identification:

a) le nom du produit faisant l'objet de l'examen;
b) le nom de la marque;
c) le nom commercial;
d) le numéro d'identification du modèle;
e) la configuration matérielle (y compris le numéro de sortie et le numéro de série);
f) l'environnement de fonctionnement ou le système d'exploitation;
g) la version du micrologiciel à l'état d'usine;
h) les informations relatives au fabricant:
   ha) le nom;
   hb) l'abréviation;
   hc) l'adresse enregistrée;
   hd) le numéro de téléphone;
   he) l'adresse e-mail;
   hf) les coordonnées de la personne de contact: le nom, la nationalité, le numéro de téléphone, l'adresse e-mail;
i) le nombre annuel prévu d'articles produits en termes de VE;
j) une indication des marchés commerciaux sur lesquels le dispositif examiné devrait être vendu au cours de la première année suivante:
   ia) la Hongrie uniquement;
   ib) les États membres de l'Union (si ce n'est pas dans l'Union dans son ensemble, la liste des États membres), ou
   ic) autres;
k) une indication du niveau d'assurance auquel l'essai sera effectué: basique/significatif/élevé.

2. Document de mise en œuvre

2.1. Le document de mise en œuvre (ci-après dénommé: «MD») contient des informations détaillées relatives à l'évaluation des exigences énoncées à l'annexe 2, qui sont utilisées dans la mise en œuvre de l'instrument IdO identifié conformément au point 1.

2.2. Contenu minimal du MD

2.2.1. MD 1-UserInfo: Informations utilisateur

Le MD répertorie la documentation, les publications et les informations fournies aux utilisateurs. L'action comprend à la fois le site internet du fabricant et l'URL correspondante, le manuel d'utilisation ou l'aide intégrée. La liste contient des informations sur le fonctionnement des fonctions et mécanismes indépendants suivants:

	A	**B**
1.	Documentation relative aux mécanismes de modification	La documentation des mécanismes de modification des valeurs d'authentification pour l'utilisateur, y compris toutes les informations nécessaires pour accéder à ladite documentation.
2.	Documentation relative au capteur	La documentation, pour l'utilisateur, sur les informations relatives aux capacités de détection externes, y compris toutes les informations nécessaires pour accéder à ladite documentation.
3.	Documentation relative au paramètre sécurisé	La méthodologie de documentation de l'utilisateur pour la configuration sécurisée de la VE, y compris toutes les informations nécessaires pour accéder à ladite documentation.
4.	Documentation relative à la vérification de la configuration	Une description de la manière dont la méthode de vérification de la configuration sécurisée de la VE est documentée pour l'utilisateur, y compris toutes les informations nécessaires pour accéder à ladite documentation.
5.	Documentation relative aux données à caractère personnel	La manière dont les informations relatives au traitement des données à caractère personnel sont documentées pour l'utilisateur, y compris toutes les informations nécessaires pour accéder à ladite documentation.
6.	Documentation relative aux données de télémétrie	La manière dont les informations relatives à la collecte des données de télémétrie sont documentées pour l'utilisateur, y compris toutes les informations nécessaires pour accéder à ladite documentation.
7.	Documentation relative à la suppression	Une description, pour l'utilisateur, de la manière dont les données personnelles sont supprimées, y compris toutes les informations nécessaires pour accéder à ladite documentation.
8.	Nom du modèle	Une indication du modèle de la VE et une brève

		description de la manière dont la désignation du modèle de la VE peut être reconnue par l'utilisateur. Préciser ici si le numéro de version de la VE et ses composants logiciels peuvent être récupérés au moyen d'une requête réseau et comment y parvenir. Si un logiciel libre est utilisé, les versions du noyau et de l'application du système d'exploitation libre et leur temps d'assistance à long terme (LTS) doivent être indiqués ici.
9.	Période de prise en charge	La période pendant laquelle le produit ou le service fait l'objet d'une maintenance par le fabricant, par exemple sous forme de mises à jour, y compris les versions du noyau et de l'application des systèmes d'exploitation libres.
10.	Publication de la période d'assistance	La manière dont la période d'assistance est publiée et documentée pour l'utilisateur, y compris toutes les informations sur l'accès à ladite publication.
11.	Divulgation en matière de vulnérabilité	La manière dont les vulnérabilités sont divulguées, y compris toutes les informations sur l'accès à ladite divulgation.
12.	Publication relative aux composants non modernisables	Une description des motifs de l'absence de mises à jour logicielles, y compris toutes les informations nécessaires pour accéder à ladite publication.

2.3.2. MD 2-SecDev: Processus de développement sûrs

Le MD répertorie tous les processus de développement sécurisés que le fabricant a effectués ou a mis en œuvre pour VE. Le MD contient les entrées suivantes:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque processus, en commençant par SecDev-1.
2.	Description	Une brève description du processus de développement sécurisé. Si une norme existante est utilisée, une référence à la norme correspondante est fournie. Une description des techniques de programmation appliquées devrait être incluse pour démontrer qu'elles sont appropriées pour limiter les attaques de piratage, de panne et de fuite.

2.3.3. MD 3-VulnTypes: Vulnérabilités pertinentes

Le MD répertorie tous les types de vulnérabilité qui sont pertinents pour la VE. Le MD comprend les entrées suivantes:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque vulnérabilité, en commençant par

		VulnTypes-1.
2.	Description	Une brève description de la vulnérabilité pertinente pour la VE.
3.	Mesure	Lorsque la vulnérabilité est détectée, une description de la manière dont les mesures sont prises en relation avec ce type de vulnérabilité, y compris toutes les organisations impliquées dans la mesure et leurs responsabilités.
4.	Délai	Une échéance dédiée dans laquelle des étapes spécifiques de la mesure sont programmées en cas de vulnérabilité. Exemple: cinq jours pour la première réponse et 90 jours avant la publication de la correction.

2.3.4. MD 4-Conf: Déclarations, prises de position

Le MD répertorie les prises de position pour les différents processus. Le MD contient les entrées indépendantes suivantes, pour lesquelles des réponses claires, OUI ou NON, doivent être indiquées.

	A	**B**
1.	Confirmation des mesures relatives à la vulnérabilité	La confirmation que l'infrastructure nécessaire est disponible pour chaque «mesure» décrite dans MD 3-VulnTypes et que les opérateurs ont été informés afin d'atteindre l'objectif «délai».
2.	Confirmation de la surveillance de la vulnérabilité	Confirmation que l'infrastructure nécessaire est en place pour surveiller, identifier et corriger chaque vulnérabilité décrite dans MD 5-VulnMon et que les opérateurs ont été informés.
3.	Confirmation des procédures de mise à jour	Confirmation que l'infrastructure nécessaire est disponible pour chaque processus de mise à jour décrit dans MD 6-UpdProc et que les opérateurs ont été informés pour atteindre le «délai» ciblé.
4.	Confirmation d'une gestion sécurisée	Confirmation que les processus de gestion sécurisés décrits dans MD 15-SecMgmt ont été établis.
5.	Confirmation d'un développement sûr	Confirmation que les processus de développement sûr décrits dans MD 2-SecDev ont été établis.

2.3.5. MD 5-VulnMon: Surveillance de la vulnérabilité

Le MD répertorie toutes les procédures de vérification, d'identification et de correction des vulnérabilités, avec les entrées suivantes:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque procédure, en commençant par VulnMon-1.
2.	Description	Une description de la manière de suivre, d'identifier et de corriger les failles de sécurité dans les produits et services.

2.3.6. MD 6-UpdProc: Procédures de mise à jour

Le MD répertorie les procédures du fabricant pour la délivrance des mises à jour de sécurité, avec les données suivantes:

	A	B
1.	Identifiant	Un identifiant unique pour chaque procédure, en commençant par UpdProc-1.
2.	Description	Une brève description de la procédure de délivrance des mises à jour de sécurité, y compris toutes les organisations et responsabilités.
3.	Délai	L'échéance prévue pour l'achèvement de la procédure.

2.3.7. MD 7-Intf: Interfaces

Le MD répertorie toutes les interfaces réseau, physiques et logiques de la VE, avec les paramètres suivants:

	A	B
1.	Identifiant	Un identifiant unique pour chaque interface, en commençant par Intf-1.
2.	Description	Une description de l'interface, y compris son but. Dans le cas d'interfaces physiques, il est également essentiel de décrire si l'interface est toujours indispensable, ou si elle n'est nécessaire que dans certains cas comme spécifié dans la description (par exemple, utilisation intermittente) ou si elle n'est jamais nécessaire.
3.	Type	Indiquer si l'interface est de type réseau, physique (y compris les interfaces sans fil), logique ou de type multiple.
4.	Statut	Indiquer si l'interface est activée ou désactivée dans l'état initialisé. Dans le cas d'interfaces autorisées, une explication est requise.
5.	Changement de statut	Une liste d'états de l'interface, indiquant comment et avec quel rôle les changements d'état peuvent être déclenchés par l'utilisateur, citant le rôle conformément à MD 9-Role.
6.	Structure du rapport	Description de la manière dont l'interface construit la connexion, quels mécanismes de validation et d'authentification elle utilise, en référence au mécanisme d'authentification MD-10-Auth.
7.	Informations publiées	Si l'interface est une interface réseau: une description des informations divulguées dans l'état initialisé sans authentification et les motifs de leur divulgation, ainsi qu'une indication de la pertinence de la divulgation aux fins de la sécurité de l'information.
8.	Interface de débogage	Si l'interface est une interface physique: si l'interface peut être utilisée comme interface de débogage.
9.	Protection	Si l'interface est une interface physique: description des méthodes de protection nécessaires pour limiter l'exposition de l'interface. Dans le cas des interfaces de débogage, il est nécessaire de décrire le mécanisme logiciel utilisé pour désactiver l'interface.

2.3.8. MD 8-DevID: Identifiants du dispositif

Tous les identifiants de VE utilisés pour identifier le dispositif sont inclus dans le MD.

	A	B
1.	Identifiant	Un identifiant unique pour chaque identifiant de dispositif, en commençant par DevID-1.
2.	Type d'identifiant	Informations sur la forme de l'identifiant (étiquette, identifiant physique ou logique) et son caractère unique.
3.	Accessibilité de l'identifiant	Avec quel rôle et comment l'identifiant peut-il être identifié par l'utilisateur dans chaque état du dispositif (emballé à l'usine, par défaut d'usine et paramètre). S'il est disponible via l'interface d'identification, il est fait référence à l'interface MD 7-Intf.
4.	Source de l'identifiant	«Préinstallé» ou «peut être ajouté par l'utilisateur».
5.	Mécanisme de génération d'identifiants	Une brève description de l'algorithme qui est utilisé pour générer l'identifiant, décrivant les actions pour s'assurer, d'une manière proportionnelle aux risques, que les identifiants réduisent le risque d'attaques automatiques qui s'appuient sur des régularités évidentes, des chaînes communes, des informations accessibles au public ou une complexité insuffisante.
6.	Exécution des opérations	Une description des opérations qui peuvent être effectuées en connaissance de cause de l'identifiant et de la manière dont elles sont effectuées, en référence aux interfaces MD 7-Intf impliquées dans l'opération.
7.	Objectifs de sécurité	Une description des objectifs de sécurité atteints et des menaces auxquelles le mécanisme devrait faire face.
8.	Protection contre la force brute	Si l'identifiant est accessible directement à partir d'une interface réseau, une description de la méthode conçue pour empêcher l'attaquant d'obtenir les données d'identification à travers une attaque par force brute via les interfaces réseau.
9.	Protection contre les attaques temporelles	Si l'identifiant est disponible directement à partir d'une interface réseau, une description de la méthode conçue pour empêcher l'attaquant d'obtenir une autorisation frauduleuse à travers des attaques temporelles.

2.3.9. MD 9-Role: Rôles

Le MD inclut les rôles traités par la VE à l'état d'usine, y compris les acteurs non soumis à l'identification et même les connexions de machine à machine.

	A	B
1.	Identifiant	Un identifiant unique pour chaque rôle, en commençant par Role-1.
2.	Description	Une brève description du rôle.
3.	Objectif	L'objectif général des utilisateurs dans le rôle.
4.	Opérations	Une liste d'actions qui peuvent être effectuées par les utilisateurs dans le rôle.

2.3.10. MD 10-AuthMech: Mécanismes d’authentification

Tous les mécanismes d’authentification de la VE sont inclus dans le MD. Le MD comprend les entrées suivantes:

	A	B
1.	Identifiant	Un identifiant unique pour chaque mécanisme d’authentification, en commençant par AuthMech-1.
2.	Description	Une brève description du mécanisme d’authentification et du processus d’autorisation associé. Préciser si le mécanisme est utilisé pour l’authentification utilisateur ou l’authentification de machine à machine et si l’on peut y accéder directement à partir d’une interface réseau. Dans le cas d’une mise en œuvre par un tiers, il convient d’expliquer comment la conception de la chaîne d’approvisionnement empêche la fuite des informations d’identification spécifiques à la VE.
3.	Facteur d’authentification	Type d’attribut utilisé pour l’authentification Pour les mots de passe, il est également nécessaire d’indiquer si le mot de passe est défini et utilisé par l’utilisateur à l’état initialisé.
4.	Mécanisme de génération de mots de passe	Si le facteur d’authentification est un mot de passe qui n’est pas défini par l’utilisateur, une description du mécanisme de génération des mots de passe, notant qu’aucune description détaillée n’est requise. La description précise si le mot de passe est unique par dispositif et s’il est préinstallé, il décrit les actions qui garantissent que les mots de passe sont uniques pour chaque dispositif dans un état autre que celui de défaut d’usine et qu’ils réduisent le risque d’attaques automatiques qui s’appuient sur des régularités évidentes, des chaînes communes, des informations accessibles au public ou une complexité inappropriée lorsque lesdits mots de passe sont utilisés comme mots de passe préinstallés et uniques par dispositif.
5.	Garanties de sécurité	Une description des objectifs de sécurité atteints et des menaces auxquelles le mécanisme devrait faire face.
6.	Détails cryptographiques	Une description des méthodes cryptographiques (protocoles, opérations, primitives, modes et tailles de clés) utilisées pour fournir le mécanisme d’authentification et faciliter les «garanties de sécurité» décrites, en prenant en considération la gestion des clés.
7.	Protection contre la force brute	Si le mécanisme d’authentification est disponible directement à partir d’une interface réseau, une description de la méthode conçue pour empêcher l’attaquant d’obtenir des détails d’authentification à travers une attaque par force brute via les interfaces réseau.
8.	Protection contre les attaques temporelles	Si le mécanisme d’authentification est disponible directement à partir d’une interface réseau, une description de la méthode conçue pour empêcher l’attaquant d’obtenir une autorisation non frauduleuse à travers des attaques temporelles.
9.	Personnalisation	Réglage des options associées au mécanisme d’authentification

10.	Application	Les rôles des interfaces et des utilisateurs utilisant le mécanisme d'authentification, en référence aux interfaces MD 7-Intf et aux rôles MD 9-Role.
11.	Manipulation	Description du processus de modification de l'identifiant d'authentification.

2.3.11. MD 11-Account: Gestion de compte

Le MD inclut des solutions liées à la gestion des comptes d'utilisateurs.

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque action et solution, en commençant par Account-1.
2.	Opération	Nom de l'opération
3.	Description	Une description détaillée du mécanisme de l'opération effectuée.
4.	Configuration	Une description des données qui peuvent être configurées dans l'opération de gestion de compte pour les utilisateurs avec quel type de rôles MD 9-Role.

2.3.12. MD 12-SoftComp: Composants logiciels

Le MD répertorie tous les composants logiciels de la VE. Le niveau de détail appliqué pour diviser le logiciel examiné en composants logiciels vise à identifier quels composants peuvent être mis à jour et lesquels ne peuvent pas être mis à jour dans le cas d'un test de vulnérabilité. Le MD contient les entrées suivantes:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque composant logiciel, à commencer par SoftComp-1.
2.	Description	Une brève description du composant logiciel. Veuillez indiquer séparément si la mise à jour du composant logiciel contient des données sensibles.
3.	Mécanisme de mise à jour	Référence aux mécanismes de mise à jour MD 13-UpdMech qui sont utilisés pour mettre à jour le composant logiciel. Une liste vide de mécanismes de mise à jour indique l'échec des mises à jour des composants logiciels et l'absence de telles mises à jour doit être justifiée.
4.	Utilisation cryptographique	Ceci indique si le composant logiciel utilise des algorithmes cryptographiques ou des primitives (oui/non) et, dans l'affirmative, si le fabricant a pris en considération les effets secondaires de la mise à jour desdits algorithmes et primitives (oui/non).

2.3.13. MD 13-UpdMech: Mécanismes de mise à jour

Le MD répertorie tous les mécanismes de mise à jour de la VE, pour lesquels les entrées suivantes sont incluses:

	A	B
1.	Identifiant	Un identifiant unique pour chaque mécanisme de mise à jour, en commençant par UpdMech-1.
2.	Description	Une brève description du mécanisme de mise à jour, y compris ses principales caractéristiques. En outre, il est nécessaire de préciser si la livraison de la mise à jour est basée sur le réseau.
3.	Garanties de sécurité	Une description des objectifs de sécurité atteints et des menaces auxquelles le mécanisme doit faire face. En outre, dans un souci d'authenticité et d'intégrité, il est nécessaire d'indiquer si la garantie de sécurité est fournie par la VE elle-même.
4.	Détails cryptographiques	Une description des méthodes cryptographiques (protocoles, opérations, primitives, modes et tailles de clés) utilisées pour assurer la sécurité du mécanisme de mise à jour de la gestion des clés et pour faciliter les «garanties de sécurité». Méthode d'installation des clés publiques à des fins de vérification.
5.	Initiation et interaction	Une brève description de la manière dont la mise à jour est lancée et une brève description de l'interaction utilisateur nécessaire pour lancer et appliquer la mise à jour, indiquant s'il s'agit d'un mécanisme de mise à jour automatique.
6.	Configuration	Une brève description de la manière dont l'utilisateur peut configurer l'automatisation et la notification des mises à jour logicielles et quelles options (par exemple autorisation, blocage, report) l'utilisateur peut choisir. La configuration par défaut doit également être spécifiée ici.
7.	Contrôle des mises à jour	Une brève description du mécanisme de requête et du calendrier pour la disponibilité des mises à jour de sécurité et si la disponibilité de la mise à jour de sécurité est vérifiée par la VE elle-même.
8.	Notification de l'utilisateur	Une brève description de la manière dont l'utilisateur est informé de la mise à jour disponible et des perturbations causées par le mécanisme de mise à jour, par exemple la disponibilité limitée de certaines fonctionnalités, en indiquant les informations contenues dans la notification et si la notification est mise en œuvre par la VE elle-même.
9.	Gestion des versions	Une brève description de la manière dont la VE vérifie et valide la version de mise à jour avant l'installation.

2.2.14. MD 14-SecParam: Paramètres de sécurité

Le MD répertorie tous les paramètres de sécurité sensibles (publics et critiques) qui sont stockés en permanence sur la VE lors d'une utilisation normale, avec les paramètres suivants:

	A	B
1.	Identifiant	Un identifiant unique pour chaque paramètre, en commençant par SecParam-1.

2.	Description	Une brève description du paramètre de sécurité, y compris son but, indiquant que le paramètre de sécurité est un identifiant unique codé en dur utilisé dans le dispositif à des fins de sécurité et qu'il est codé en dur dans le code source du logiciel du dispositif.
3.	Lieu de stockage	Emplacement et méthode de stockage du paramètre de sécurité
4.	Type	Noter si le paramètre de sécurité est public ou critique.
5.	Garanties de sécurité	Une description des objectifs de sécurité de base atteints et des menaces contre lesquelles le paramètre de sécurité est protégé pendant le stockage à long terme.
6.	Système de protection	Une description des mesures prises pour atteindre les garanties de sécurité, y compris les autorisations et les rôles par lesquels l'accès au paramètre est possible, ainsi que les droits associés à chaque rôle.
7.	Mécanisme d'attribution	Si le «type» indique que le paramètre est critique: une description du mécanisme par lequel le paramètre reçoit une valeur.
8.	Mécanismes de communication	Une référence aux mécanismes de communication utilisés dans MD 16-ComMech pour communiquer les paramètres et une indication si la communication a lieu via des interfaces accessibles à distance.
9.	Mécanisme de création	Si le «type» indique que le paramètre est critique ou qu'il est utilisé pour vérifier l'intégrité et l'authenticité des mises à jour logicielles ou pour protéger la communication avec les services connexes: une description du mécanisme utilisé pour créer des valeurs pour le paramètre et, en outre, une indication que le paramètre est utilisé pour vérifier l'intégrité et l'authenticité des mises à jour logicielles ou pour protéger la communication avec les services connexes.

2.2.15. MD 15-SecMgmt: Processus de gestion sûrs

Le MD répertorie chaque processus de gestion sûr des paramètres de sécurité critiques que le fabricant a mis en œuvre pendant le cycle de vie de la VE:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque processus, en commençant par SecMgmt-1.
2.	Description	Une brève description du processus de gestion de la sécurité pour l'ensemble du cycle de vie des paramètres de sécurité critiques, en référence à la norme correspondante lorsqu'une norme existante est utilisée. Le cycle de vie des paramètres de sécurité critiques tient généralement compte de la génération, de la fourniture, du stockage, des mises à jour, de l'extraction, de l'archivage, de la destruction, des processus d'expiration et de la vulnérabilité des paramètres. Au cours de la génération, la méthode de production des nombres aléatoires utilisés et la mesure de son entropie doivent également être décrites. S'il existe une vérification de l'intégrité du fichier, il convient également

		de décrire comment elle est mise en œuvre.

2.2.16. MD 16-ComMech: Mécanismes de communication

Le MD répertorie tous les mécanismes de communication de la VE, avec les informations détaillées suivantes:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque mécanisme, en commençant par ComMech-1.
2.	Description	Une brève description du mécanisme de communication, y compris son objet et une description du protocole utilisé. Pour les protocoles standardisés, la référence avec un numéro de version est suffisante. En outre, il convient d'indiquer si le mécanisme est disponible à distance.
3.	Garanties de sécurité	Une description des objectifs de sécurité atteints et des menaces auxquelles le mécanisme doit faire face.
4.	Détails cryptographiques	Une description des méthodes cryptographiques utilisées pour fournir le mécanisme de communication (protocoles, opérations, primitives, modes et tailles de clés), en prenant en considération la gestion des clés, afin d'atteindre les objectifs des «garanties de sécurité» décrites.
5.	Mesures de résilience	Une description des mesures visant à s'assurer que la relation est établie de manière ordonnée, y compris l'état attendu, opérationnel et stable menant à la réalisation d'une relation stable.

2.2.17. MD 17-NetSecImpl: Mises en œuvre du réseau et de la sécurité

Le MD répertorie toutes les mises en œuvre des fonctions réseau et de sécurité de la VE.

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque élément, en commençant par NetSecImpl-1.
2.	Description	Une brève description de la mise en œuvre du réseau ou de la fonction de sécurité, y compris son objet et sa portée.
3.	Méthode d'examen/d'évaluation	Une description de la méthodologie utilisée pour examiner ou évaluer la mise en œuvre, y compris les principes de base (par exemple, l'audit, l'examen par les pairs, l'analyse automatique du code) et une description de la portée de la mise en œuvre couverte par la méthodologie.
4.	Rapport	Le résultat de l'examen ou de l'évaluation, ou une référence au certificat ou au rapport d'évaluation démontrant que la mise en œuvre a été jugée réussie.

2.2.18. MD 18-SoftServ: Services logiciels

Le MD répertorie tous les services logiciels de la VE, comme suit:

	A	B
1.	Identifiant	Un identifiant unique pour chaque service, en commençant par SoftServ-1.
2.	Description	Une brève description du service, y compris son but, indiquant si le service est disponible,si oui à travers quelle interface réseau MD 7-Intf et si c'est également le cas à l'état initialisé.
3.	Statut	Une indication que le service est activé ou désactivé à l'état initialisé.
4.	Justification	Si le service est autorisé, expliquer pourquoi le service est nécessaire à l'utilisation ou au bon fonctionnement de la VE.
5.	Configuration	Si le service est disponible via une interface réseau: des informations sur la question de savoir si le service permet une modification de configuration pertinente pour la sécurité et, dans l'affirmative, une brève description de la configuration possible. Dans le cas d'un composant logiciel tiers, une déclaration indiquant que le service est désactivé par défaut.
6.	Mécanisme d'authentification	Si le service est disponible via une interface réseau: référence dans MD 10-AuthMech aux mécanismes d'authentification utilisés pour l'authentification avant d'utiliser le service.
7.	SW d'un tiers	Une indication si le composant logiciel provient d'un tiers. Dans l'affirmative, une description de la procédure de séparation.

2.2.19. MD 19-CodeMin: Minification des codes

Le MD répertorie les méthodes utilisées pour minifier les codes:

	A	B
1.	Identifiant	Un identifiant unique pour chaque méthode, en commençant par CodeMin-1.
2.	Description	Une brève description de la méthode utilisée pour minifier le code à la fonctionnalité requise.

2.2.20. MD 20-PrivlCtrl: Contrôle des droits

Le MD répertorie tous les mécanismes de contrôle des droits, comme suit:

	A	B
1.	Identifiant	Un identifiant unique pour chaque mécanisme, en commençant par PrivlCtrl-1.
2.	Description	Une brève description du mécanisme de vérification des droits et autorisations pour les rôles et le logiciel sur la VE.
3.	Matrice	La matrice d'autorisation gérée par le mécanisme de contrôle des droits respectif.
4.	Authentification	Référence au mécanisme d'authentification requis par le mécanisme de contrôle des droits respectif.

2.2.21. MD 21-AccCtrl: Protection des accès

Le MD répertorie les mécanismes de protection des accès à la mémoire au niveau matériel, comme suit.

	A	B
1.	Identifiant	Un identifiant unique pour chaque mécanisme, en commençant par AccCtrl-1.
2.	Description	Une brève description du mécanisme de contrôle des accès au niveau matériel, y compris la manière dont le système d'exploitation de la VE le prend en charge.

2.2.22. MD 22-SecBoot: Mécanismes de démarrage du système sécurisés

Le MD répertorie tous les mécanismes de démarrage sécurisés de la VE, comme suit:

	A	B
1.	Identifiant	Un identifiant unique pour chaque mécanisme, en commençant par SecBoot-1.
2.	Description	Une brève description du mécanisme utilisé pour le processus de démarrage sécurisé de la VE (y compris les hypothèses de sécurité) et l'identification de la partie protégée du logiciel. Une attention particulière devrait être accordée à toutes les options de contrôle, les appels API qui affectent le fonctionnement du mécanisme. Si la VE utilise une sauvegarde du logiciel protégé, son utilisation est également incluse dans la description.
3.	Garanties de sécurité	Une description des objectifs de sécurité mis en œuvre par le mécanisme. Les mécanismes mettent en œuvre l'authenticité et l'intégrité des noyaux des systèmes d'exploitation.
4.	Mécanismes de détection	Une description du mécanisme de détection de la modification non autorisée du logiciel de la VE.
5.	Notification de l'utilisateur	Une brève description de la manière dont l'utilisateur est informé de toute modification non autorisée du logiciel, en tant qu'informations supplémentaires, indiquant quelles informations sont contenues dans la notification.
6.	Fonctionnalités de notification	Une brève description des fonctionnalités réseau requises pour la notification de l'utilisateur.

2.2.23. MD 23-Store: Stockage et restauration

Le MD répertorie la manière dont les données traitées par la VE sont stockées et comment les données peuvent être restaurées, comme suit:

	A	B
1.	Identifiant	Un identifiant unique pour chaque méthode de stockage, en commençant par Store-1.
2.	Produit de stockage	La méthode et le lieu de stockage des données traitées par la VE.
3.	Redondance	En cas de défaillance du mécanisme de stockage, son mécanisme de remplacement.
4.	La méthode de restauration des données	La manière dont les données historiques sont restaurées en cas de défaillance du stockage primaire ou de VE.
5.	Chiffrement	L'algorithme de cryptage utilisé sur le produit de stockage, indiquant si le chiffrement est activé à l'état par défaut d'usine, et comment et avec quel rôle le stockage crypté peut-il être configuré par l'utilisateur.

2.2.24. MD 24-DataSec: Protection des données

Le MD répertorie toutes les données traitées par la VE, à l'exception des données de télémétrie, comme suit:

	A	B
1.	Identifiant	Un identifiant unique pour chaque donnée, en commençant par DataSec-1.
2.	Description	Une brève description de la catégorie de données traitées par la VE. Les données personnelles sont des informations sur toute personne physique identifiée ou identifiable.
3.	Activités de traitement	Une description du traitement des données, décrivant toutes les parties concernées et les finalités pour lesquelles les données sont traitées.
4.	Mécanismes de communication:	Référence aux mécanismes de communication MD 16-ComMech utilisés pour communiquer les données et indiquant si le partenaire de communication est un service associé (oui/non). Une liste vide de mécanismes de communication indique que les données ne sont pas transmises.
5.	Sensibilité	Une indication précisant si les données sont des données sensibles. Les données sensibles sont toutes les données dont la divulgation est susceptible de causer un préjudice à la personne concernée. Les données considérées comme sensibles peuvent varier en fonction du produit et de l'utilisation, mais les exemples incluent les informations de paiement, le contenu des données de communication et les données de localisation horodatées.
6.	Obtenir un consentement	Si des données à caractère personnel sont traitées sur la base du consentement de la personne concernée: une description de la façon dont le consentement est obtenu.
7.	Retrait d'un consentement	Lorsque des données à caractère personnel sont traitées sur la base du consentement de la personne concernée: une description de la manière dont la personne concernée peut retirer son consentement au traitement

		des données à caractère personnel.
8.	Protection cryptographique	L'algorithme cryptographique utilisé pour protéger les données personnelles, en référence à MD 12-SoftComp.
9.	Produit de stockage	Produit(s) de stockage pour le stockage de données, selon MD 23-Store.

2.2.25. MD 25-ExtSens: Capteurs externes

Le MD répertorie toutes les capacités de détection externes de la VE, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque capteur, à commencer par ExtSens-1.
2.	Description	Une brève description de la capacité de détection.

2.2.26. MD 26-ResMech: Mécanismes de résilience

Le MD répertorie tous les mécanismes de résilience pour la déconnexion du réseau ou la panne de courant de la VE, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque mécanisme, en commençant par ResMech-1.
2.	Description	Une description du mécanisme de résilience qui contribue à la résilience de la VE aux pannes de réseau et d'électricité.
3.	Type	Le mécanisme de résilience est utilisé pour gérer les perturbations de la connexion au réseau ou une panne de courant, ou pour gérer les deux.
4.	Garanties de sécurité	Une description des objectifs de sécurité atteints et des menaces auxquelles le mécanisme devrait faire face.

2.2.27. MD 27-TelData: Données de télémétrie

Le MD répertorie toutes les données de télémétrie collectées par la VE, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque donnée, en commençant par TelData-1.
2.	Description	Une brève description des données de télémétrie collectées par la VE et fournies au fabricant.
3.	Objectif	Une brève description des finalités pour lesquelles les données sont collectées.
4.	Test de sécurité	Si les données sont utilisées pour des tests de sécurité, une description de la manière dont et par qui (dispositif ou service connexe) sont examinées des données de télémétrie pour des troubles de sécurité.
5.	Connexions de	Référence dans MD 24-DataSec aux données traitées dans les données de

	données	télémétrie.

2.2.28. MD 28-DelFunc: Fonctionnalités de suppression

Le MD répertorie toutes les fonctionnalités de suppression des données de l'utilisateur, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque fonctionnalité de suppression, en commençant par DelFunc-1.
2.	Description	Une brève description de la fonction utilisée pour supprimer les données de l'utilisateur. Si le «type cible» indique qu'il s'agit d'un service connexe, le service connexe couvert par la fonction est également indiqué.
3.	Type cible	Indiquer si la fonction s'applique aux données de l'utilisateur sur le dispositif ou aux données à caractère personnel traitées dans les services connexes, ou les deux.
4.	Initiation et interaction	Une brève description de l'interaction utilisateur qui est nécessaire pour démarrer et appliquer la fonctionnalité de suppression.
5.	Confirmation	Une brève description de la manière dont l'utilisateur reçoit une indication que les données concernées ont été supprimées, après l'application de la fonctionnalité de suppression.

2.2.29. MD 29-UserDec: Décisions des utilisateurs

Le MD répertorie toutes les décisions à prendre lors de l'installation et de la maintenance, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque décision, en commençant par UserDec-1.
2.	Description	Une description des décisions à prendre par l'utilisateur dans le cadre des processus d'installation et de maintenance, y compris le rôle de l'utilisateur dans le processus d'installation ou de maintenance.
3.	Options	Une description des options pertinentes pour la sécurité parmi lesquelles l'utilisateur peut faire son choix et une indication de la valeur par défaut.
4.	Décision	Une brève description de la manière dont la décision est prise, précisant si la décision peut également être prise par l'utilisateur final.

2.2.30. MD 30-UserIntf: Interfaces utilisateur

Le MD répertorie toutes les interfaces utilisateur de la VE qui permettent l'entrée de l'utilisateur, comme suit:

	A	**B**

1.	Identifiant	Un identifiant unique pour chaque interface, en commençant par UserIntf-1.
2.	Description	Une description du but, de la fonction et des champs d'entrée de l'interface utilisateur permettant à ce dernier d'entrer des données, expliquant également comment l'utilisateur peut accéder à l'interface.
3.	Interface de configuration	Une indication précisant si l'interface peut être utilisée pour la configuration de la VE.
4.	Mécanisme de communication	S'il est possible d'utiliser l'interface pour la configuration de la VE, alors une référence aux mécanismes de communication dans MD 16-ComMech, qui est utilisée pour protéger l'interface.

2.2.31. MD 31-ExtAPI: API externes

Le MD répertorie toutes les API de VE qui permettent l'entrée de données à partir de sources externes, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque API, en commençant par ExtAPI-1.
2.	Description	Une description de l'API de VE permettant l'entrée de sources externes. Les API externes sont généralement utilisées pour la communication de machine à machine.

2.2.32. MD 32-InpVal: Validation de l'entrée des données

Le MD répertorie toutes les méthodes de validation d'entrée de données de VE, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque méthode, en commençant par InpVal-1.
2.	Description	Une description de la méthode utilisée pour valider les données saisies par l'intermédiaire d'interfaces utilisateur ou transmises par l'intermédiaire d'API ou entre les réseaux dans les services et dispositifs, y compris la gestion de données inattendues. Il est également nécessaire de préciser quelles sources d'entrée de données sont ciblées par la méthode. Afin de valider l'entrée des données, il est possible de vérifier si les données sont du type admissible (format et structure), de la valeur admissible, du nombre ou de l'ordre autorisé.

2.2.33. MD 33-Notif: Notifications

Le MD inclut tous les modes de notification des utilisateurs, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque méthode de notification, en

		commençant par Notif-1.
2.	Mode de notification	Une description de l’interface MD 7-Intf sur laquelle la notification apparaît et à quels utilisateurs.
3.	Gestion des notifications	Actions à effectuer par l’utilisateur dans le cadre de la notification.
4.	Table des matières	Le contenu des notifications si elles peuvent être configurées, une description du rôle de MD 9-Role avec lequel l’utilisateur peut configurer le contenu des données et à quelle profondeur.

2.2.34. MD 34-AuditLog: Données relatives à l’enregistrement

Le MD répertorie toutes les méthodes d’enregistrement de VE, comme suit:

	A	**B**
1.	Identifiant	Un identifiant unique pour chaque élément d’enregistrement, en commençant par AuditLog-1.
2.	Description	La portée de l’activité d’enregistrement, le contenu des enregistrements.
3.	Garanties de sécurité	Une description des objectifs de sécurité de base atteints et des menaces contre lesquelles les données des enregistrements sont protégées pendant le stockage à long terme.
4.	Système de protection	Une description des mesures entreprises pour atteindre les garanties de sécurité, décrivant les autorisations et les rôles par lesquels l’accès au paramètre est possible, y compris les droits associés à chaque rôle.

3. Document qui sous-tend l’évaluation

3.1. Le fabricant délivre un document d’évaluation qui prouve le respect des exigences énoncées à l’annexe 2, en ce qui concerne le niveau d’assurance pour la VE soumise à l’essai (ci-après dénommé: «EMD»).

3.2. Le document comprend une liste des exigences énoncées à l’annexe 2 pour le niveau d’assurance cible, ainsi que les informations suivantes:

a) la classification du fabricant: la déclaration de conformité du fabricant à la présente exigence. Elle peut avoir les valeurs suivantes:

aa) «Sans objet»: ceci peut être utilisé si l’exigence n’est pas applicable en ce qui concerne la VE, et que la conception physique, les fonctions prévues et le domaine d’utilisation de la VE ne permettent pas de satisfaire à la présente exigence.

ab) «Applicable et respectée»: ceci peut être utilisé si l’exigence relative à la VE est applicable et que la VE satisfait à la présente exigence.

b) méthode d’exécution: Dans le cas du marquage «applicable et respecté», une description des composants inclus dans le MD en ce qui concerne l’exigence et la manière dont ils satisfont à l’exigence, individuellement ou ensemble.

c) justification: Dans le cas du marquage «sans objet», l’exposé des motifs, compte tenu de l’ensemble des circonstances.

Ensemble d'exigences

1. En ce qui concerne les exigences de sécurité, les exigences qui doivent être respectées par le dispositif défini dans le document d'identification du dispositif IdO à l'annexe 1, point 1, par niveau d'assurance, sont spécifiées dans les colonnes C à E.

2. Les exigences ont été élaborées sous réserve des normes européennes et nationales suivantes:
   a) ETSI EN 303 645 V2.1.1;
   b) publication spéciale 800-213A du NIST et;
   c) publication spéciale 800-53 du NIST, Révision 5.

3. Dans n'importe quelle colonne:
   a) les lignes marquées par «-» indiquent les noms des familles de contrôle;
   b) «X» indique que le respect de l'exigence de sécurité dans ladite ligne est obligatoire au niveau d'assurance spécifié dans les colonnes C à E;
   «0» indique que le respect de l'exigence de sécurité dans ladite ligne n'est pas obligatoire au niveau d'assurance spécifié dans les colonnes C à E.

	A	B	C	D	E
1.	**Identifiant**	**Description**	**basique**	**significatif**	**élevé**
2.		IDENTIFICATION DU DISPOSITIF	-	-	-
3.		Identification du dispositif	-	-	-
4.	DEVID-1	Le marquage du modèle du dispositif IdO est clairement reconnaissable, que ce soit sur l'étiquette du dispositif ou via une interface physique.	X	X	X
5.	DEVID-2	Le dispositif IdO dispose d'un identifiant logique unique qui peut être récupéré via une interface ou peut être trouvé sur le dispositif même.	X	X	X
6.	DEVID-3	Il est possible de définir l'identifiant unique et le marquage du modèle d'un dispositif IdO qui peut être contrôlé à distance.	X	X	X
7.	DEVID-4	L'outil IdO offre la possibilité d'ajouter un identifiant physique unique auquel les entités autorisées peuvent accéder.	0	X	X

8.		Exécution des opérations			
9.	DEVOP-1	L'outil IdO est capable d'effectuer des opérations qui peuvent se produire lors de l'identification ou de l'utilisation du dispositif.	X	X	X
10.	DEVOP-2	L'outil IdO est capable de faire la distinction entre les utilisateurs identifiés et non identifiés.	X	X	X
11.	DEVOP-3	Les utilisateurs non autorisés ne peuvent pas prendre connaissance de l'identifiant logique unique du dispositif IdO.	0	X	X
12.	DEVOP-4	Connaissant l'identifiant du dispositif IdO, la version actuelle du logiciel peut être vérifiée.	0	X	X
13.	DEVOP-5	Aux fins de l'identification et de la gestion des périphériques réseau, l'identifiant du dispositif peut être utilisé pour détecter le dispositif IdO.	0	0	X
14.		Prise en charge de l'identification du dispositif	-	-	-
15.	IDSUPP-1	L'outil IdO est capable de se faire de la publicité auprès d'autres actifs en tant qu'entité préidentifiée.	0	X	X
16.	IDSUPP-2	La vérification de l'authenticité des autres dispositifs IdO est assurée.	0	X	X
17.	IDSUPP-3	Dans le cas des connexions réseau et distantes, le dispositif IdO effectue une identification bidirectionnelle cryptographique avant de construire la connexion identifiée.	0	0	X
18.	IDSUPP-4	L'outil IdO prend en charge l'identification et l'authentification basées sur des certificats.	0	0	X
19.		CONFIGURATION DU DISPOSITIF	-	-	-
20.	DEVCONF-1	Le réglage des droits d'accès logiques, la configuration du dispositif IdO,conformément aux exigences sur les «connexions externes, contrôle de l'interface», ne sont possibles que par le biais d'utilisateurs privilégiés.	X	X	X
21.	DEVCONF-2	Seuls les utilisateurs autorisés peuvent configurer la politique d'identification des dispositifs IdO et les listes de restrictions d'accès conformément aux exigences sur les «connexions externes, contrôle de l'interface».	X	X	X
22.	DEVCONF-3	Seuls les utilisateurs autorisés peuvent configurer les interfaces logiques et physiques du dispositif IdO, conformément aux exigences sur les «connexions externes, contrôle de l'interface».	X	X	X
23.	DEVCONF-4	Les utilisateurs autorisés peuvent configurer les paramètres logiciels du dispositif IdO.	X	X	X
24.	DEVCONF-5	Les utilisateurs autorisés peuvent restaurer le dispositif IdO à son statut d'usine.	X	X	X
25.	DEVCONF-6	Les utilisateurs autorisés peuvent restaurer le dispositif IdO dans un état sécurisé précédent autre que l'état d'usine.	0	0	X
26.	DEVCONF-7	Le statut de configuration précédent est assuré pendant ou après l'entretien, la réparation du dispositif IdO.	0	X	X
27.		PROTECTION DES DONNÉES	-	-	-
28.		Support cryptographique	-	-	-

29.	CRYPT-1	L'outil IdO fournit un algorithme cryptographique d'une force et d'une efficacité suffisantes pour protéger les données.	X	X	X
30.	CRYPT-2	L'outil IdO est capable de valider des certificats individuels.	0	X	X
31.	CRYPT-3	La vérification de la signature numérique est assurée.	0	X	X
32.	CRYPT-4	L'outil IdO peut exécuter des algorithmes de hachage.	X	X	X
33.	CRYPT-5	Ils peuvent être mis à jour aux versions recommandées des algorithmes cryptographiques et des primitives.	0	X	X
34.	CRYPT-6	Le code source du dispositif ne contient pas de paramètres de sécurité critiques codés en dur.	0	X	X
35.	CRYPT-7	Les paramètres de sécurité critiques, qui sont utilisés pour vérifier l'intégrité et l'authenticité des mises à jour logicielles et pour protéger les communications dans les logiciels du dispositif avec les services connexes, sont uniques pour chaque dispositif et sont produits avec un mécanisme qui réduit le risque d'attaques automatisées.	X	X	X
36.		Prise en charge des clés cryptographiques	-	-	-
37.	CRYKEY-1	Le dispositif IdO gère les clés cryptographiques en toute sécurité.	X	X	X
38.	CRYKEY-2	Le dispositif IdO est capable de générer des paires de clés.	X	X	X
39.	CRYKEY-3	Le dispositif IdO stocke les clés cryptographiques en toute sécurité.	X	X	X
40.	CRYKEY-4	Le dispositif IdO apporte des modifications aux clés cryptographiques en toute sécurité.	X	X	X
41.	CRYKEY-5	Le dispositif IdO vérifie les clés cryptographiques générées par des systèmes externes.	0	X	X
42.		Stockage sûr	-	-	-
43.	SECSTR-1	Le dispositif IdO ne stocke pas et ne transmet pas de mots de passe, à l'exclusion du stockage de la valeur de hachage générée à partir du mot de passe avec la fonctionnalité de fractionnement cryptographique irréversible.	X	X	X
44.	SECSTR-2	Le stockage en toute sécurité peut être autorisé par l'intermédiaire du dispositif IdO ou de son interface.	X	X	X
45.	SECSTR-3	À l'état d'usine, le stockage sécurisé, sûr et crypté des données est autorisé.	X	X	X
46.	SECSTR-4	La protection des données à caractère personnel est assurée conformément au 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).	X	X	X
47.	SECSTR-5	Le dispositif IdO, y compris l'infrastructure cloud qui garantit l'accès aux données, ne stocke que la quantité de données nécessaire à son fonctionnement opérationnel.	X	X	X
48.	SECSTR-6	Le dispositif IdO peut stocker des données cryptées localement.	X	X	X

49.	SECSTR-7	Les éléments du système à distance liés au dispositif IdO (par exemple, le cloud) stockent les données sous une forme cryptée.	0	X	X
50.	SECSTR-8	Les paramètres de sécurité sensibles sont stockés dans un stockage persistant.	0	X	X
51.	SECSTR-9	Les données du système et de l'utilisateur sont placées sur des partitions séparées.	0	X	X
52.	SECSTR-10	Une sauvegarde sécurisée des données est assurée.	0	X	X
53.	SECSTR-11	Les données de l'utilisateur stockées localement sur le dispositif IdO peuvent être facilement et irrémédiablement supprimées.	X	X	X
54.	SECSTR-12	Les données de l'utilisateur stockées par des éléments du système à distance associés au dispositif IdO peuvent être facilement supprimées.	0	X	X
55.		Transfert sécurisé de données	-	-	-
56.	SECDT-1	Le flux de données sur les interfaces d'entrée et de sortie du dispositif IdO est sécurisé.	X	X	X
57.	SECDT-2	L'algorithme cryptographique pour la transmission sécurisée des données peut être configuré.	0	X	X
58.	SECDT-3	Le dispositif IdO est protégé contre l'accès et la modification non autorisés dans l'environnement de connexion de données.	X	X	X
59.	SECDT-4	L'outil IdO vérifie l'intégrité des données transmises et reçues en utilisant une solution cryptographique.	0	X	X
60.		ACCÈS LOGIQUE AUX INTERFACES	-	-	-
61.		Prise en charge de l'identification	-	-	-
62.	AUTH-1	L'outil IdO prend en charge les méthodes d'authentification.	X	X	X
63.	AUTH-2	L'outil IdO est capable d'exiger une méthode d'authentification pour construire des connexions, en particulier dans le cas des connexions à distance.	X	X	X
64.	AUTH-3	Pour des populations d'utilisateurs spécifiques, l'outil IdO prend en charge une méthode d'authentification multifactorielle.	0	X	X
65.	AUTH-4	Si votre dispositif IdO utilise des mots de passe par défaut d'usine, ils sont uniques pour chaque dispositif.	0	X	X
66.	AUTH-5	Lors de la génération de mots de passe par défaut d'usine, l'outil IdO utilise un algorithme de génération qui réduit le risque d'attaques automatiques.	0	X	X
67.	AUTH-6	La modification d'un identifiant correspondant au mécanisme d'authentification utilisé est simplement assurée à l'utilisateur.	X	X	X
68.	AUTH-7	L'outil IdO masque les données pendant le processus d'authentification.	X	X	X
69.	AUTH-8	L'outil IdO prend en charge une méthode d'authentification standardisée et uniforme (par exemple, SAML, OAuth2).	0	X	X

70.	AUTH-9	Pour l'accès à distance, le dispositif IdO vérifie les données d'authentification par opération.	0	0	X
71.	AUTH-10	En fournissant une rétroaction masquée des informations contenues dans la rétroaction de la méthode d'authentification, le dispositif IdO garantit que les identifiants d'authentification ne sont pas connus et ne peuvent pas être réutilisés par des personnes non autorisées.	X	X	X
72.		Configuration de l'identification	-	-	-
73.	IDENT-1	Tout au long du cycle de vie du dispositif IdO, les méthodes, les règles et les restrictions d'authenticité peuvent être définies et modifiées.	0	X	X
74.	IDENT-2	L'outil IdO prend en charge la gestion des comptes de manière automatisée.	0	0	X
75.	IDENT-3	Le nombre de tentatives d'identification échouées peut être configuré, après quoi le dispositif IdO interdit l'accès à l'utilisateur pour une durée de temps définie.	0	X	X
76.	IDENT-4	L'outil IdO prend en charge la restauration d'un compte qui est interdit en raison de tentatives d'identification infructueuses avec une méthode d'identification alternative.	0	0	X
77.	IDENT-5	L'outil IdO fournit une rétroaction sur la date de la dernière authentification réussie.	0	X	X
78.	IDENT-6	L'outil IdO prend en charge la déconnexion des comptes inactifs, dont la durée peut être configurée.	X	X	X
79.	IDENT-7	Le dispositif IdO interdit automatiquement les comptes d'utilisateurs temporaires d'une manière qui peut être configurée.	0	X	X
80.	IDENT-8	L'outil IdO enregistre les tentatives de connexion infructueuses, qui peuvent être signalées.	X	X	X
81.	IDENT-9	Le dispositif IdO indique le nombre de tentatives de connexion infructueuses à l'utilisateur lors de la prochaine connexion réussie.	0	X	X
82.	IDENT-10	L'outil IdO prend en charge l'authentification des utilisateurs et systèmes externes.	X	X	X
83.	IDENT-11	L'accès aux comptes d'utilisateurs, aux utilisateurs externes et aux systèmes peut être révoqué, auquel cas le dispositif IdO détruit la connexion existante.	0	X	X
84.	IDENT-12	L'outil IdO prend en charge la définition d'une date d'expiration pour les comptes, ce qui garantira que le compte est bloqué au-delà de la date d'expiration.	0	X	X
85.		Notification de l'utilisateur	-	-	-
86.	NOTIF-1	Le statut du dispositif IdO peut être facilement identifié visuellement en vérifiant les indicateurs de statut.	X	X	X
87.	NOTIF-2	Les informations affichées sur l'écran du dispositif IdO peuvent être configurées.	0	X	X
88.	NOTIF-3	L'outil IdO peut envoyer (de manière configurée) des notifications aux utilisateurs.	X	X	X
89.	NOTIF-4	L'intégralité du contenu des notifications contenant des données personnelles et des notifications de sécurité ne peut être divulguée qu'après identification et les données sensibles ne seront pas affichées dans	0	X	X

		le message d'alerte.			
90.	NOTIF-5	Le contenu des messages affichés par le dispositif IdO peut être configuré.	0	X	X
91.	NOTIF-6	Si le message d'alerte apparaît sur l'écran du dispositif IdO, celui-ci garantit que le message reste sur l'écran jusqu'à l'interaction de l'utilisateur.	0	X	X
92.		Prise en charge de la gestion des accès	-	-	-
93.	ACCESS-1	Le dispositif IdO résiste aux opérations non autorisées.	X	X	X
94.	ACCESS-2	Le dispositif IdO est capable d'identifier les utilisateurs et les processus autorisés (par exemple, les systèmes de connexion).	X	X	X
95.	ACCESS-3	Le dispositif IdO fait la distinction entre les utilisateurs autorisés et non autorisés.	X	X	X
96.	ACCESS-4	Certaines fonctions qui peuvent être définies par l'opérateur sont disponibles sans identification.	X	X	X
97.		Prise en charge et gestion des rôles	-	-	-
98.	ROLE-1	Le dispositif IdO peut gérer plusieurs types de comptes d'utilisateurs.	X	X	X
99.	ROLE-2	Le dispositif IdO séparera au moins les types de comptes d'utilisateurs suivants: les comptes personnels (général et privilégié), les comptes privilégiés scindés.	0	X	X
100.	ROLE-3	L'outil IdO prend en charge l'ajout de comptes d'utilisateurs.	0	X	X
101.	ROLE-4	Les rôles peuvent être attribués aux comptes d'utilisateurs.	0	X	X
102.	ROLE-5	Les comptes d'utilisateurs sont fournis avec un identifiant unique.	0	X	X
103.	ROLE-6	L'outil IdO effectue un contrôle d'accès logique basé sur les rôles.	0	X	X
104.	ROLE-7	Les fonctionnalités et les processus auxquels un utilisateur administrateur peut accéder avec les rôles peuvent être configurés.	0	X	X
105.	ROLE-8	Les rôles sont compatibles avec les méthodes d'autorisation standardisées et unifiées, la correspondance peut être configurée (par exemple, LDAPS).	0	X	X
106.	ROLE-9	Un utilisateur administrateur peut configurer un nouveau rôle.	0	0	X
107.	ROLE-10	Par défaut, les rôles sont conçus selon le principe de l'autorisation minimale.	X	X	X
108.	ROLE-11	La configuration de la gestion des accès à l'historique et aux paramètres de sécurité est prise en charge.	0	X	X
109.	ROLE-12	L'outil IdO vous permet de définir des conditions restrictives pour chaque type d'utilisateur (par exemple, restriction basée sur le temps, limite IP).	0	0	X
110.	ROLE-13	Les autorisations et droits attribués aux rôles sont vérifiés dans le cas d'interactions utilisateur visant à créer des fonctionnalités et des processus privilégiés.	0	0	X
111.	ROLE-14	Les méthodes d'authentification utilisées pour les différents comptes utilisateur peuvent être configurées.	0	0	X

112.	ROLE-15	Dans le cas de comptes fractionnés, l'autorisation de connexion simultanée peut être configurée par compte (interdit à l'état d'usine).	0	X	X
113.	ROLE-16	Le dispositif IdO est capable d'appliquer des restrictions prédéfinies lors de l'utilisation du dispositif.	0	X	X
114.		Connexions externes, contrôle de l'interface	-	-	-
115.	INTCTRL-1	Le dispositif IdO fournit une connexion à des systèmes tiers externes avec l'utilisation d'une méthode sécurisée.	X	X	X
116.	INTCTRL-2	L'utilisation de composants du dispositif IdO peut être restreinte (ports, fonctionnalités, périphériques d'entrée et de sortie).	X	X	X
117.	INTCTRL-3	Les interfaces physiques ou logiques qui ne sont pas nécessaires au fonctionnement du dispositif IdO peuvent être désactivées.	X	X	X
118.	INTCTRL-4	Seules les interfaces physiques et logiques minimales requises pour l'installation et la mise en service sont autorisées à l'état par défaut d'usine.	X	X	X
119.	INTCTRL-5	À l'état par défaut d'usine, le dispositif IdO protège contre la récupération d'informations de sécurité sans identification.	X	X	X
120.	INTCTRL-6	Le matériel n'expose pas les interfaces physiques à des risques inutiles.	0	X	X
121.	INTCTRL-7	L'utilisation des services de l'outil IdO peut être restreinte.	0	X	X
122.	INTCTRL-8	L'accès externe à l'interface de gestion peut être désactivé.	0	X	X
123.	INTCTRL-9	L'accès aux interfaces logiques du dispositif IdO peut être contrôlé.	X	X	X
124.	INTCTRL-10	Le dispositif IdO prend en charge la connexion sans fil, dont le protocole d'authentification sécurisé et autorisé peut être configuré.	X	X	X
125.	INTCTRL-11	Si votre dispositif IdO dispose d'une interface de débogage, celle-ci est interdite par le logiciel.	0	X	X
126.		MISE À JOUR LOGICIELLE	-	-	-
127.		Capacités de mise à jour	-	-	-
128.	UPD-1	Le logiciel du dispositif IdO peut être mis à jour en toute sécurité comme prévu par le logiciel ou via une interface.	X	X	X
129.	UPD-2	La mise à jour du logiciel peut être effectuée avec un compte utilisateur identifié et autorisé, pris en charge par un mécanisme sécurisé et pouvant être configuré.	0	X	X
130.	UPD-3	La version actuelle du logiciel du dispositif IdO peut être consultée.	X	X	X
131.	UPD-4	Les comptes autorisés peuvent restaurer le logiciel à une version antérieure.	0	X	X

132.	UPD-5	Les mises à jour logicielles proviennent d'une source faisant autorité et la conformité à la présente condition est vérifiée par le dispositif IdO.	X	X	X
133.	UPD-6	Les mises à jour logicielles n'entraînent pas une diminution de la préparation en matière de cybersécurité du dispositif IdO, et l'outil IdO dispose d'une méthode intégrée pour vérifier la présente exigence.	0	X	X
134.		Gestion des mises à jour grâce à la prise en charge des applications	0	0	0
135.	UPDCTRL-1	L'outil IdO vérifie l'authenticité et l'intégrité des mises à jour.	X	X	X
136.	UPDCTRL-2	Il est possible de désactiver la mise à jour automatique du dispositif IdO.	X	X	X
137.	UPDCTRL-3	Les méthodes de mise à jour manuelle et automatique sont prises en charge.	X	X	X
138.	UPDCTRL-4	La méthode de mise à jour peut être sélectionnée.	X	X	X
139.	UPDCTRL-5	Le logiciel vérifie la disponibilité d'une nouvelle mise à jour à des intervalles qui peuvent être spécifiés.	X	X	X
140.	UPDCTRL-6	Les nouvelles versions logicielles sont notifiées par le dispositif IdO, mais cette fonctionnalité peut être désactivée.	X	X	X
141.	UPDCTRL-7	Les nouvelles versions logicielles sont notifiées par le dispositif IdO et la portée de celles à notifier peut être configurée.	0	0	X
142.	UPDCTRL-8	Le dispositif IdO informe l'utilisateur si la mise à jour présente un risque pour le fonctionnement essentiel du dispositif.	0	X	X
143.		PRISE EN CHARGE DE LA GESTION D'ÉVÉNEMENTS	-	-	-
144.		Enregistrement	-	-	-
145.	LOG-1	L'outil IdO est capable d'enregistrer des événements.	X	X	X
146.	LOG-2	Le dispositif IdO prend en charge une connexion au système d'enregistrement externe.	0	X	X
147.	LOG-3	Le contenu minimal des entrées de l'enregistrement est le suivant: l'identifiant unique du dispositif IdO, le signal temporel, la source de l'événement, le type d'événement, la classification de l'événement, l'identifiant de l'utilisateur ou l'identificateur de processus, la description de l'événement.	0	X	X
148.	LOG-4	Le dispositif IdO est capable d'enregistrer les communications réseau.	0	X	X
149.	LOG-5	Le dispositif IdO est capable d'enregistrer les modifications dans la configuration du dispositif.	0	X	X
150.	LOG-6	Le dispositif IdO est capable d'enregistrer les tentatives d'accès réussies et infructueuses.	X	X	X
151.	LOG-7	Le dispositif IdO est capable d'enregistrer son propre statut et celui de ses capteurs.	0	X	X
152.	LOG-8	En fonction de la liste des événements qui peuvent être enregistrés, les événements à enregistrer peuvent être configurés.	0	0	X
153.	LOG-9	Le statut du dispositif IdO peut être consulté via l'interface.	0	X	X

154.	LOG-10	Vous pouvez définir le temps de conservation maximal des événements, le nombre d'événements de journaux stockés et la taille maximale du fichier journal.	0	X	X
155.	LOG-11	La suppression complète des fichiers journaux au-delà des critères de conservation sur le dispositif IdO est assurée.	0	X	X
156.		Gestion du signal temporel	-	-	-
157.	TIMESTP-1	La signalisation temporelle des événements enregistrés par le dispositif IdO est exacte à quelques secondes près.	0	X	X
158.	TIMESTP-2	Le dispositif IdO prend en charge un protocole réseau NTP.	0	X	X
159.	TIMESTP-3	Une horloge fiable peut être configurée.	0	X	X
160.	TIMESTP-4	Le dispositif IdO utilise un signal horaire standard qui peut être retracé à l'UTC.	0	X	X
161.		Prise en charge de la gestion d'événements	-	-	-
162.	INC-1	Le dispositif IdO envoie une alerte sur les incidents configurés qui sont considérés comme des incidents de sécurité.	0	X	X
163.	INC-2	Le dispositif IdO envoie une alerte sur les incidents configurés qui sont considérés comme des incidents de sécurité aux systèmes d'information associés.	0	0	X
164.	INC-3	Le mode d'alerte peut être configuré.	0	0	X
165.	INC-4	L'outil IdO prend en charge une solution d'enregistrement alternative en cas de défaillance du mécanisme d'enregistrement principal.	0	0	X
166.		SÉCURITÉ DES ACTIFS	-	-	-
167.		Communication sécurisée	-	-	-
168.	SECCOM-1	L'initiation et la fermeture d'une connexion avec d'autres dispositifs se font en toute sécurité.	X	X	X
169.	SECCOM-2	Le dispositif IdO est capable d'appliquer les règles de gestion du trafic.	0	X	X
170.	SECCOM-3	Le dispositif IdO utilise des protocoles standardisés pendant la communication.	X	X	X
171.	SECCOM-4	L'adresse IP du dispositif IdO peut être définie.	X	X	X
172.	SECCOM-5	Les ports des interfaces du dispositif IdO peuvent être configurés.	0	X	X
173.	SECCOM-6	Le dispositif IdO dispose d'une prise en charge DNS.	X	X	X
174.		Utilisation sûre des ressources	-	-	-
175.	RESRC-1	L'outil IdO est capable de partager des ressources.	0	X	X
176.	RESRC-2	Le dispositif IdO peut affecter des zones de mémoire aux processus.	0	X	X
177.	RESRC-3	Les différents processus n'atteignent pas la zone de mémoire attribuée à un autre processus.	0	X	X

178.	RESRC-4	La zone de mémoire n’est accessible que par le noyau.	0	X	X
179.	RESRC-5	La mémoire est protégée par un contrôle d’accès basé sur le matériel.	0	X	X
180.	RESRC-6	Des quotas peuvent être attribués à l’utilisation de disques.	0	0	X
181.	RESRC-7	En cas de perte de connexion au réseau, un fonctionnement limité est assuré.	X	X	X
182.	RESRC-8	Le dispositif IdO prend en charge le stockage de données compressées.	0	0	X
183.		Protection de l’intégrité	-	-	-
184.	INT-1	Le dispositif IdO est protégé contre l’exécution d’un code unique à partir d’une source non autorisée.	0	X	X
185.	INT-2	Le dispositif IdO a la capacité de détecter les modifications matérielles et logicielles indésirables.	0	X	X
186.	INT-3	Le dispositif IdO dispose d’une fonctionnalité de contrôle de la conformité de sécurité pour la configuration de base.	0	X	X
187.	INT-4	Le dispositif IdO dispose d’une fonctionnalité de contrôle d’intégrité.	0	X	X
188.	INT-5	L’outil IdO vérifie son logiciel en utilisant des mécanismes sécurisés de démarrage du système.	0	X	X
189.	INT-6	Si le dispositif IdO détecte des modifications non autorisées du logiciel, il alerte l’utilisateur ou l’administrateur du problème et ne se connecte pas à des réseaux plus larges que ceux requis pour la fonctionnalité d’alerte.	0	X	X
190.	INT-7	L’outil IdO est capable de détecter les manipulations pendant le cycle de vie du développement du système.	0	0	X
191.	INT-8	L’environnement d’exécution est stocké sur un support en lecture seule.	0	X	X

Exigences affectées par les tests de vulnérabilité

Un test de vulnérabilité est effectué au cours de l'évaluation pour les exigences suivantes de l'annexe 2:

	A	B
1.	**Identifiant**	**Description**
2.	DEVID-3	Il est possible de définir l'identifiant unique et le marquage du modèle d'un dispositif IdO qui peut être contrôlé à distance.
3.	DEVID-4	L'outil IdO devrait prévoir la possibilité d'ajouter un identifiant physique unique auquel les entités autorisées ont accès.
4.	DEVOP-3	Les utilisateurs non autorisés ne peuvent pas prendre connaissance de l'identifiant logique unique du dispositif IdO.
5.	IDSUPP-2	La vérification de l'authenticité des autres dispositifs IdO est assurée.
6.	IDSUPP-3	Dans le cas des connexions réseau et distantes, le dispositif IdO effectue une identification bidirectionnelle cryptographique avant de construire la connexion identifiée.
7.	IDSUPP-4	L'outil IdO prend en charge l'identification et l'authentification basées sur des certificats.
8.	DEVCONF-1	La configuration des droits d'accès logiques, la configuration du dispositif IdO, telle que décrite à l'article sur les «accès logiques aux interfaces», n'est possible que par le biais d'utilisateurs privilégiés.
9.	DEVCONF-2	Seuls les utilisateurs autorisés peuvent configurer la stratégie d'identification des dispositifs IdO et les listes de restrictions d'accès. Comme décrit à l'article sur les «accès logiques aux interfaces».
10.	DEVCONF-3	Seuls les utilisateurs autorisés peuvent configurer les interfaces logiques et physiques du dispositif IdO, conformément à l'article sur les«accès logiques aux interfaces».
11.	CRYPT-1	L'outil IdO fournit un algorithme cryptographique d'une force et d'une efficacité suffisantes pour protéger les données.

12.	CRYPT-2	L’outil IdO est capable de valider des certificats individuels.
13.	CRYPT-3	La vérification de la signature numérique est assurée.
14.	CRYPT-4	L’outil IdO peut exécuter des algorithmes de hachage.
15.	CRYPT-6	Le code source du dispositif ne contient pas de paramètres de sécurité critiques codés en dur.
16.	CRYPT-7	Les paramètres de sécurité critiques, qui sont utilisés pour vérifier l’intégrité et l’authenticité des mises à jour logicielles et pour protéger la communication avec les services connexes dans le logiciel du dispositif, sont uniques pour chaque dispositif et fabriqués avec un mécanisme qui réduit le risque d’attaques automatisées contre les classes d’actifs.
17.	CRYKEY-1	Le dispositif IdO gère les clés cryptographiques en toute sécurité.
18.	CRYKEY-2	Le dispositif IdO est capable de générer des paires de clés.
19.	CRYKEY-3	Le dispositif IdO stocke les clés cryptographiques en toute sécurité.
20.	CRYKEY-4	Le dispositif IdO apporte des modifications aux clés cryptographiques en toute sécurité.
21.	CRYKEY-5	Le dispositif IdO vérifie les clés cryptographiques générées par des systèmes externes.
22.	SECSTR-1	Le dispositif IdO ne stocke pas et ne transmet pas de mots de passe, à l’exclusion du stockage de la valeur de hachage générée à partir du mot de passe avec la fonctionnalité de fractionnement cryptographique irréversible.
23.	SECSTR-4	La protection des données à caractère personnel est assurée conformément au 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).
24.	SECDT-3	Le dispositif IdO est protégé contre l’accès et la modification non autorisés dans l’environnement de connexion de données.
25.	SECDT-4	L’outil IdO vérifie l’intégrité des données transmises et reçues en utilisant une solution cryptographique.

26.	AUTH-3	Pour des populations d'utilisateurs spécifiques, l'outil IdO prend en charge une méthode d'authentification multifactorielle.
27.	AUTH-5	Lors de la génération de mots de passe par défaut d'usine, l'outil IdO utilise un algorithme de génération qui réduit le risque d'attaques automatiques.
28.	AUTH-7	L'outil IdO masque les données pendant le processus d'authentification.
29.	AUTH-8	L'outil IdO prend en charge une méthode d'authentification standardisée et uniforme (par exemple, SAML, OAuth2).
30.	AUTH-9	Pour l'accès à distance, le dispositif IdO vérifie les données d'authentification par opération.
31.	AUTH-10	En fournissant une rétroaction masquée des informations contenues dans la rétroaction de la méthode d'authentification, le dispositif IdO garantit que les identifiants d'authentification ne sont pas connus et ne peuvent pas être réutilisés par des personnes non autorisées.
32.	IDENT-10	L'outil IdO prend en charge l'authentification des utilisateurs et systèmes externes.
33.	NOTIF-4	L'intégralité du contenu des notifications contenant des données personnelles et des notifications de sécurité ne peut être divulguée qu'après identification et les données sensibles ne seront pas affichées dans le message d'alerte.
34.	ACCESS-1	Le dispositif IdO résiste aux opérations non autorisées.
35.	ROLE-12	L'outil IdO vous permet de définir des conditions restrictives pour chaque type d'utilisateur (par exemple, restriction basée sur le temps, limite IP).
36.	INTCTRL-2	L'utilisation de composants du dispositif IdO peut être restreinte (ports, fonctionnalités, périphériques d'entrée et de sortie).
37.	INTCTRL-3	Les interfaces physiques ou logiques qui ne sont pas nécessaires au fonctionnement du dispositif IdO peuvent être désactivées.
38.	INTCTRL-4	Seules les interfaces physiques et logiques minimales requises pour l'installation et la mise en service sont autorisées à l'état par défaut d'usine.
39.	INTCTRL-5	À l'état par défaut d'usine, le dispositif IdO protège contre la récupération d'informations de sécurité sans identification.
40.	INTCTRL-8	L'accès externe à l'interface de gestion peut être désactivé.

41.	INTCTRL-9	L’accès aux interfaces logiques du dispositif IdO peut être contrôlé.
42.	INTCTRL-10	Le dispositif IdO prend en charge la connexion sans fil, dont le protocole d’authentification sécurisé et autorisé peut être configuré.
43.	INTCTRL-11	Si votre dispositif IdO dispose d’une interface de débogage, celle-ci est interdite par le logiciel.
44.	UPD-4	Les comptes autorisés peuvent restaurer le logiciel à une version antérieure. (par exemple, attaque de rétrogradation).
45.	UPD-5	Les mises à jour logicielles proviennent d’une source faisant autorité et la conformité à la présente condition est vérifiée par le dispositif IdO.
46.	SECCOM-2	Le dispositif IdO est capable d’appliquer les règles de gestion du trafic.
47.	RESRC-3	Les différents processus n’atteignent pas la zone de mémoire attribuée à un autre processus.
48.	RESRC-4	La zone de mémoire n’est accessible que par le noyau.
49.	RESRC-5	La mémoire est protégée par un contrôle d’accès basé sur le matériel.
50.	INT-1	Le dispositif IdO est protégé contre l’exécution d’un code unique à partir d’une source non autorisée.
51.	INT-2	Le dispositif IdO a la capacité de détecter les modifications matérielles et logicielles indésirables.
52.	INT-4	Le dispositif IdO dispose d’une fonctionnalité de contrôle d’intégrité.
53.	INT-5	L’outil IdO vérifie son logiciel en utilisant des mécanismes sécurisés de démarrage du système.
54.	INT-6	Si le dispositif IdO détecte des modifications non autorisées du logiciel, il alerte l’utilisateur ou l’administrateur du problème et ne se connecte pas à des réseaux plus larges que ceux requis pour la fonctionnalité d’alerte.

Annexe 4 du décret nº …/2024 (… …) de l'autorité de surveillance des affaires réglementaires (SZTFH)

Méthodologie de l'évaluation

1. Le dispositif IdO à tester

1.1. La VE à tester est un outil IdO spécifique qui devrait être évalué conformément aux dispositions du présent système de certification. Le fabricant ou l'organisme d'évaluation de la conformité qui effectue l'évaluation est en mesure de contrôler la VE par l'intermédiaire des interfaces disponibles et, sur la base des informations fournies dans le MD, est partiellement au courant de sa conception (boîtes de tests grises). La VE est en état de fonctionnement pendant l'évaluation et d'autres services connexes sont opérationnels même s'ils ne sont pas vérifiés par le fabricant ou par l'organisme d'évaluation de la conformité.

2. Document qui sous-tend l'évaluation

2.1. L'EMD mentionné à l'annexe 1 est préparé par le fabricant en ce qui concerne les capacités mises en œuvre et prises en charge dans la VE, conformément aux dispositions du présent système de certification. Dans l'EMD, le fabricant déclare que toutes les exigences énoncées à l'annexe 2 pour le niveau d'assurance examiné ont été respectées.

3. Document de mise en œuvre

3.1. Le fabricant prépare un MD comme indiqué à l'annexe 1, qui contient des informations supplémentaires et plus détaillées pour effectuer l'évaluation. Le MD constitue une base sous-jacente à la méthodologie d'évaluation et comprend certains détails de conception pour l'organisme d'évaluation de la conformité.

3.2. Le fabricant fournit des informations complètes, détaillées et correctes lors du remplissage du MD.

3.3. Lorsqu'il remplit le MD, le fabricant peut également se référer à la documentation existante, auquel cas il met la documentation de référence à la disposition de l'organisme d'évaluation de la conformité.

4. Les fonctions et obligations du fabricant

4.1. Le fabricant, en tant qu'organisation à l'origine de l'évaluation, demande l'examen d'une VE donnée dans le cadre du présent système de certification. Le fabricant sera le point de contact unique de l'organisme d'évaluation de la conformité et sera responsable de la coordination avec les parties impliquées dans la chaîne d'approvisionnement et l'écosystème de la VE, en particulier les fabricants de composants, les fournisseurs de services et les développeurs d'applications.

4.2. Les évaluations par des tiers des certificats de sécurité existants ou des parties de VE peuvent être utilisées en partie comme preuve de conformité afin de réduire les ressources et le temps nécessaires à l'évaluation. Dans le présent cas, le fabricant indique dans l'EMD que la conformité a déjà été évaluée, accompagné d'une référence aux éléments de preuve

appropriés. En outre, le fabricant fournit à l'organisme d'évaluation de la conformité toutes les informations nécessaires à la vérification des preuves, en particulier les détails de la certification et les rapports d'évaluation. Au cours de l'évaluation, l'organisme d'évaluation de la conformité vérifie que les éléments de preuve sont en mesure de démontrer le respect de l'exigence énoncée dans ladite annexe 2.

5. Fonctions et obligations de l'organisme d'évaluation de la conformité

5.1. Le laboratoire d'essai impliqué par l'organisme d'évaluation de la conformité procède à l'évaluation de la conformité de la VE. L'évaluation tient également compte des liens avec les services connexes et des processus de développement et de gestion de la VE. Dans le cas d'autoévaluations de la conformité, aux fins du point 6, l'organisme d'évaluation de la conformité s'entend comme le fabricant.

6. La procédure d'évaluation

6.1. Les étapes du processus d'évaluation sont les suivantes:

6.2. Pour chacune des exigences désignées comme «applicables et respectées» dans l'EMD, un organisme d'évaluation de la conformité enregistre les cas d'essai conformément au point 7, élabore un plan d'essai pour la VE et réalise les essais.

6.2. Pour chacune des exigences indiquées dans l'EMD, plusieurs cas d'essai sont testés conformément aux points 6.2.1 à 6.2.5.

6.2.1. Cas d'essai: <*Identifiant de l'exigence*>-*T0 – Applicabilité*

L'objectif de l'essai:
Le présent cas d'essai a pour objet d'évaluer l'applicabilité d'une exigence spécifique énoncée à l'annexe 2.

Unités d'essai:

a) Un organisme d'évaluation de la conformité vérifie que le fabricant a désigné l'exigence comme étant «applicable et respectée».
b) Lorsque l'exigence a été classée comme étant «applicable et respectée», un organisme d'évaluation de la conformité examine si le fabricant a indiqué la méthode de performance.
c) Lorsque l'exigence a été classée comme étant «sans objet», l'organisme d'évaluation de la conformité examine et évalue sa justification.

Décision:
Une décision de la qualification «réussi» peut être prise si:

- Dans le cas de la qualification «applicable et respectée», la «méthode d'exécution» a été achevée.
- Dans le cas de la qualification «sans objet», l'exposé des motifs est fondé.

Dans le cas contraire, la décision prise est la qualification «échec».

6.2.2. Cas d'essai: <*Identifiant de l'exigence*>-*T1 – Documentation*

Prérequis:

L’exigence énoncée à l’annexe 2 est «applicable et respectée» conformément à l’EMD et le cas d’essai précédent (<Identifiant de l’exigence>-T0) est évalué comme étant «réussi».

L’objectif de l’essai:
L’objectif du présent cas d’essai est d’établir qu’une exigence spécifique de l’annexe 2 est documentée. Le cas d’essai est applicable à tous les niveaux d’assurance.

Unités d’essai:

> Un organisme d’évaluation de la conformité vérifie que la conformité à l’exigence a été dûment documentée par le fabricant, en identifiant les éléments MD qui peuvent être utilisés pour démontrer la conformité à ladite exigence.

Décision:
Une décision de la qualification «réussi» peut être prise si le MD contient toutes les informations pertinentes concernant l’exigence.
Dans le cas contraire, la décision prise est la qualification «échec».

6.2.3. Cas d’essai: *<Identifiant de l’exigence>-T2 – Test conceptuel*

Prérequis:
L’exigence énoncée à l’annexe 2 est «applicable et respectée» conformément à l’EMD et le cas d’essai précédent (<Identifiant de l’exigence>-T1) est évalué comme étant «réussi».

L’objectif de l’essai:
L’objectif du présent cas d’essai est d’établir la conformité conceptuelle du respect de l’exigence de l’annexe 2 de la documentation. Le cas d’essai est applicable à tous les niveaux d’assurance.

Unités d’essai:
Un organisme d’évaluation de la conformité vérifie que, sur la base des informations identifiées dans le cas d’essai <identifiant de l’exigence>-T1, la VE satisfait de manière conceptuelle à l’exigence énoncée à l’annexe 2.

Décision:
Une décision de la qualification «réussi» peut être prise si, sur la base des informations identifiées dans le cas d’essai <identifiant de l’exigence>-T1, la VE est conforme de manière conceptuelle à l’exigence énoncée à l’annexe 2 et que le contrôle et la mise en œuvre de la sécurité appliqués sont proportionnels aux risques par rapport au niveau d’assurance.
Dans le cas contraire, la décision prise est la qualification «échec».

6.2.4. Cas d’essai: *<Identifiant de l’exigence>-T3 – Test de mise en œuvre*

Prérequis:
L’exigence énoncée à l’annexe 2 est «applicable et respectée» conformément à l’EMD et le cas d’essai précédent (<Identifiant de l’exigence>-T2) est évalué comme étant «réussi».

L’objectif de l’essai:
L’objectif du présent cas d’essai est d’établir le respect de l’exigence de l’annexe 2 via la documentation. Le cas d’essai est applicable à tous les niveaux d’assurance.

Unités d'essai:
Un organisme d'évaluation de la conformité vérifie que la mise en œuvre a eu lieu conformément aux informations identifiées dans le cas d'essai <identifiant de l'exigence>-T1.

Décision:
Une décision de la qualification «réussi» peut être prise si la mise en œuvre a été effectuée sur la base des informations identifiées dans le cas d'essai <identifiant de l'exigence>-T1.
Dans le cas contraire, la décision prise est la qualification «échec».

6.2.5. Cas d'essai: *<Identifiant de l'exigence>-T4 – Test de vulnérabilité*

Prérequis:
L'exigence énoncée à l'annexe 2 est «applicable et respectée» conformément à l'EMD et le cas d'essai précédent (<Identifiant de l'exigence>-T2) est évalué comme étant «réussi».

L'objectif de l'essai:
L'objectif du présent cas d'essai est d'évaluer l'exigence énoncée à l'annexe 3 au moyen d'une méthode de test de vulnérabilité. Le cas d'essai est appliqué au moins à un niveau d'assurance «significatif».

Unités d'essai:
L'organisme d'évaluation de la conformité vérifie s'il existe une vulnérabilité connue en ce qui concerne les solutions utilisées et vérifie la réalisation de l'objectif de sécurité au moyen d'un test de vulnérabilité manuel.

Décision:
Une décision de la qualification «réussi» peut être prise si aucune vulnérabilité ne peut être identifiée sur la base du test.
Dans le cas contraire, la décision prise est la qualification «échec».

7. Résultat de l'évaluation

À la suite de l'évaluation, les résultats des cas d'essai sont enregistrés sur la base d'un cas d'essai. L'organisme d'évaluation de la conformité établit un rapport d'évaluation sur la mise en œuvre des cas d'essai, qui comprend:

- les informations enregistrées dans l'EMD;
- les identifiants du cas d'essai pour chaque exigence;
- la manière dont les cas d'essai sont évalués;
- les faits à l'origine de la décision concernant le cas d'essai;
- dans le cas d'un cas d'essai pour les tests de vulnérabilité, le rapport d'essai;
- la décision concernant le cas d'essai;
- une évaluation globale des exigences.

Évaluation de l'exigence:

- «Respectée» si tous les cas d'essai étaient liés à l'exigence «réussie»;
- L'évaluation aboutit à un résultat «non respecté» si l'un des cas d'essai était lié à l'exigence «échec».

Une déclaration de conformité ou un certificat national de cybersécurité peut être délivré si la VE est évaluée comme «réussie» pour toutes les exigences énoncées dans l'EMD.

Annexe 5 du décret nº …/2024 (… …) de l'autorité de surveillance des affaires réglementaires (SZTFH)

DÉCLARATION DE CONFORMITÉ

DÉCLARATION NATIONALE DE CONFORMITÉ EN MATIÈRE DE CYBERSÉCURITÉ

Nom du fabricant:
Adresse du fabricant:

dispositif IdO	
nom:	
numéro de version:	
numéro du modèle:	
niveau d'assurance:	

Autres spécifications techniques, normes et procédures:

Portée et restriction fondée sur les circonstances:

Durée de validité: **jour**

Je déclare que le produit décrit ci-dessus est conforme aux exigences du décret de l'autorité de surveillance des affaires réglementaires relatif au système national de certification de la cybersécurité pour les dispositifs IdO.

Par la présente, je déclare que seul(e) ***[nom du fabricant]*** **est autorisé(e) à publier la présente déclaration.**

Date d'émission: Cliquer ici pour saisir une date.

---

signature autorisée du fabricant

……

À remplir par SZTFH.

Date de l'enregistrement:	
Identifiant de l'enregistrement:	

Annexe 6 du décret nº …/2024 (… …) de l'autorité de surveillance des affaires réglementaires (SZTFH)

Certificat national de la CYBERSÉCURITÉ

CERTIFICAT NATIONAL DE LA

CYBERSÉCURITÉ

<Nom de l'organisme d'évaluation de la conformité> (adresse enregistrée), enregistré par l'autorité de surveillance des affaires réglementaires sous le numéro d'enregistrement <numéro d'enregistrement> en tant que **organisme d'évaluation de la conformité** répondant aux critères de délivrance des certificats de cybersécurité au niveau d'assurance <niveau d'assurance> conformément au décret SZTFH relatif à la certification de la cybersécurité des technologies de l'information et de la communication, **certifie** que le dispositif IdO suivant, qui a été produit par

<nom du fabricant>,

à savoir

<Nom du dispositif IdO

satisfait aux exigences énoncées dans le décret de l'autorité de surveillance des affaires réglementaires relatif au système national de certification de la cybersécurité pour les dispositifs IdO, au

<niveau d'assurance>

niveau d'assurance.

Le présent certificat a été délivré sur la base du rapport d'évaluation numéro <numéro>.

Créé pour le <nom du client> (siège social).

Durée de validité: jour

Date d'émission: Cliquer ici pour saisir une date.

---------- ----------

certificateur professionnel de l'évaluation de la conformité organisme d'évaluation de la conformité

signature légale

.....

À remplir par SZTFH.

Date de l'enregistrement:	
Identifiant de l'enregistrement:	

SZTFH

Autorité de surveillance
des affaires réglementaires

Annexe 7 du décret nº …/2024 (… …) de l'autorité de surveillance des affaires réglementaires (SZTFH)

Étiquette et marquage