Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Q.5050

(03/2019)

SÉRIE Q: COMMUTATION ET SIGNALISATION ET MESURES ET TESTS ASSOCIÉS

Lutte contre la contrefaçon et le vol d'équipements TIC

Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC

Recommandation UIT-T Q.5050

RECOMMANDATIONS UIT-T DE LA SÉRIE Q

COMMUTATION ET SIGNALISATION ET MESURES ET TESTS ASSOCIÉS

SIGNALISATION DANS LE SERVICE MANUEL INTERNATIONAL	Q.1–Q.3
EXPLOITATION INTERNATIONALE AUTOMATIQUE ET SEMI-AUTOMATIQUE	Q.4–Q.59
FONCTIONS ET FLUX D'INFORMATION DES SERVICES DU RNIS	Q.60–Q.99
CLAUSES APPLICABLES AUX SYSTÈMES NORMALISÉS DE L'UIT-T	Q.100–Q.119
SPÉCIFICATIONS DES SYSTÈMES DE SIGNALISATION N° 4, 5, 6, R1 ET R2	Q.120–Q.499
COMMUTATEURS NUMÉRIQUES	Q.500–Q.599
INTERFONCTIONNEMENT DES SYSTÈMES DE SIGNALISATION	Q.600–Q.699
SPÉCIFICATIONS DU SYSTÈME DE SIGNALISATION N° 7	Q.700–Q.799
INTERFACE Q3	Q.800–Q.849
SYSTÈME DE SIGNALISATION D'ABONNÉ NUMÉRIQUE N° 1	Q.850–Q.999
RÉSEAUX MOBILES TERRESTRES PUBLICS	Q.1000–Q.1099
INTERFONCTIONNEMENT AVEC LES SYSTÈMES MOBILES À SATELLITES	Q.1100–Q.1199
RÉSEAU INTELLIGENT	Q.1200–Q.1699
PRESCRIPTIONS ET PROTOCOLES DE SIGNALISATION POUR LES IMT-2000	Q.1700–Q.1799
SPÉCIFICATIONS DE LA SIGNALISATION RELATIVE À LA COMMANDE D'APPEL INDÉPENDANTE DU SUPPORT	Q.1900–Q.1999
RNIS À LARGE BANDE	Q.2000–Q.2999
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX DE PROCHAINE GÉNÉRATION	Q.3000–Q.3709
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX PILOTÉS PAR LOGICIEL (SDN)	Q.3710–Q.3899
SPÉCIFICATIONS DE TEST	Q.3900–Q.4099
SPÉCIFICATIONS ET PROTOCOLES DE SIGNALISATION POUR LES RÉSEAUX IMT-2020	Q.5000–Q.5049
LUTTE CONTRE LA CONTREFAÇON ET LE VOL D'ÉQUIPEMENTS TIC	**Q.5050–Q.5069**

Pour plus de détails, voir la Liste des Recommandations de l'UIT-T.

Recommandation UIT-T Q.5050

Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC

Résumé

Ces dernières années, l'utilisation d'équipements fondés sur les technologies de l'information et de la communication (TIC) dans la vie quotidienne s'est intensifiée, mais elle s'est aussi accompagnée d'effets secondaires indésirables liés à l'augmentation de la vente, de la circulation et de l'utilisation de dispositifs TIC de contrefaçon sur le marché.

Un dispositif TIC de contrefaçon est un produit qui enfreint expressément la marque de fabrique, copie les modèles de matériels et de logiciels, enfreint les droits liés à la marque ou à l'emballage d'un produit original ou authentique et, en règle générale, enfreint les normes techniques, les prescriptions réglementaires ou les procédures de conformité, les accords de licences de fabrication applicables aux niveaux national et/ou international ou les autres prescriptions juridiques applicables.

Parmi les différents types de dispositifs TIC utilisés actuellement, les smartphones et autres dispositifs mobiles sont devenus des objets omniprésents et attrayants pour la population mondiale et, par voie de conséquence, ont également attiré l'attention du marché noir et du marché gris à l'échelle mondiale.

Cette situation a des conséquences négatives pour les parties prenantes telles que les utilisateurs, les opérateurs de réseau, les fabricants de dispositifs authentiques, les négociants et les pouvoirs publics, notamment une diminution de la protection de la sécurité et de la qualité de service pour les utilisateurs, ainsi qu'un manque à gagner pour un éventail de parties prenantes.

Étant donné que le principe économique de l'offre et de la demande en ce qui concerne les dispositifs TIC de contrefaçon rend plus difficiles les initiatives prises pour lutter contre le marché mondial de la contrefaçon, aucune solution unique ne peut à elle seule résoudre le problème et il est alors nécessaire de prendre toute une série de mesures dans le cadre d'une approche globale.

Par conséquent, la Recommandation UIT-T Q.5050 vise à définir un cadre de référence, y compris les difficultés principales et les exigences de haut niveau, dont il faudrait tenir compte lors de la mise en oeuvre de solutions visant à lutter contre la circulation et l'utilisation de dispositifs TIC de contrefaçon.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T Q.5050	15-03-2019	11	11.1002/1000/13702

Mots clés

Lutte contre la contrefaçon de dispositifs TIC, conformité, évaluation de la conformité, cadre, exigences, sécurité, norme, identificateurs uniques.

* Pour accéder à la Recommandation, reporter cet URL http://handle.itu.int/ dans votre navigateur Web, suivi de l'identifiant unique, par exemple http://handle.itu.int/11.1002/1000/11830-en.

AVANT-PROPOS

L'Union internationale des télécommunications (UIT) est une institution spécialisée des Nations Unies dans le domaine des télécommunications et des technologies de l'information et de la communication (ICT). Le Secteur de la normalisation des télécommunications (UIT-T) est un organe permanent de l'UIT. Il est chargé de l'étude des questions techniques, d'exploitation et de tarification, et émet à ce sujet des Recommandations en vue de la normalisation des télécommunications à l'échelle mondiale.

L'Assemblée mondiale de normalisation des télécommunications (AMNT), qui se réunit tous les quatre ans, détermine les thèmes d'étude à traiter par les Commissions d'études de l'UIT-T, lesquelles élaborent en retour des Recommandations sur ces thèmes.

L'approbation des Recommandations par les Membres de l'UIT-T s'effectue selon la procédure définie dans la Résolution 1 de l'AMNT.

Dans certains secteurs des technologies de l'information qui correspondent à la sphère de compétence de l'UIT-T, les normes nécessaires se préparent en collaboration avec l'ISO et la CEI.

NOTE

Dans la présente Recommandation, l'expression "Administration" est utilisée pour désigner de façon abrégée aussi bien une administration de télécommunications qu'une exploitation reconnue.

Le respect de cette Recommandation se fait à titre volontaire. Cependant, il se peut que la Recommandation contienne certaines dispositions obligatoires (pour assurer, par exemple, l'interopérabilité et l'applicabilité) et on considère que la Recommandation est respectée lorsque toutes ces dispositions sont observées. Le futur d'obligation et les autres moyens d'expression de l'obligation comme le verbe "devoir" ainsi que leurs formes négatives servent à énoncer des prescriptions. L'utilisation de ces formes ne signifie pas qu'il est obligatoire de respecter la Recommandation.

DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'UIT attire l'attention sur la possibilité que l'application ou la mise en œuvre de la présente Recommandation puisse donner lieu à l'utilisation d'un droit de propriété intellectuelle. L'UIT ne prend pas position en ce qui concerne l'existence, la validité ou l'applicabilité des droits de propriété intellectuelle, qu'ils soient revendiqués par un membre de l'UIT ou par une tierce partie étrangère à la procédure d'élaboration des Recommandations.

A la date d'approbation de la présente Recommandation, l'UIT n'avait pas été avisée de l'existence d'une propriété intellectuelle protégée par des brevets à acquérir pour mettre en œuvre la présente Recommandation. Toutefois, comme il ne s'agit peut-être pas de renseignements les plus récents, il est vivement recommandé aux développeurs de consulter la base de données des brevets du TSB sous http://www.itu.int/ITU-T/ipr/.

TABLE DES MATIÈRES

Page

Recommandation UIT-T Q.5050

Cadre pour des solutions permettant de lutter contre la contrefaçon de dispositifs TIC

1 Domaine d'application

La présente Recommandation définit un cadre de référence ainsi que les exigences à prendre en compte lors de la mise en oeuvre des solutions permettant de lutter contre la circulation et l'utilisation de dispositifs fondés sur les technologies de l'information et de la communication (TIC) de contrefaçon.

2 Références

Les Recommandations UIT-T et autres références suivantes contiennent des dispositions qui, par suite de la référence qui y est faite, constituent des dispositions de la présente Recommandation. Au moment de la publication, les éditions indiquées étaient en vigueur. Toutes les Recommandations et autres références étant sujettes à révision, les utilisateurs de la présente Recommandation sont invités à rechercher la possibilité d'appliquer les éditions les plus récentes des Recommandations et autres références énumérées ci-dessous. Une liste des Recommandations UIT-T en vigueur est publiée périodiquement. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document en tant que tel le statut de Recommandation.

Aucune.

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 évaluation de la conformité [b-ISO/CEI 17000]: démonstration que des exigences spécifiées relatives à un produit, un processus, un système, une personne ou un organisme sont respectées.

3.1.2 système (ou programme) d'évaluation de la conformité [b-ISO/CEI 17000]: système portant sur l'évaluation de la conformité d'objets déterminés, soumis aux mêmes exigences, règles et procédures spécifiques.

3.1.3 surveillance du marché [b-Règlement-CE]: opérations effectuées et mesures prises par les pouvoirs publics pour garantir que les produits sont conformes aux exigences légales définies dans la législation pertinente et ne portent pas atteinte à la santé et à la sécurité ou à tout autre aspect de la protection de l'intérêt public.

3.1.4 norme [b-OMC-OTC]: document approuvé par un organisme reconnu, qui fournit, pour des usages communs et répétés, des règles, des lignes directrices ou des caractéristiques pour des produits ou des procédés et des méthodes de production connexes, dont le respect n'est pas obligatoire. Il peut aussi traiter en partie ou en totalité de terminologie, de symboles, de prescriptions en matière d'emballage, de marquage ou d'étiquetage, pour un produit, un procédé ou une méthode de production donnés.

3.1.5 surveillance [b-ISO/CEI 17000]: répétition systématique d'opérations d'évaluation de la conformité au titre desquelles il est possible de prolonger la validité de la déclaration de conformité.

3.1.6 obstacle technique au commerce [b-OMC-OTC]: l'Accord sur les obstacles techniques au commerce de l'Organisation mondiale du commerce (OMC) vise à faire en sorte que les règlements techniques, les normes et les procédures d'évaluation de la conformité soient non discriminatoires et ne créent pas d'obstacles non nécessaires au commerce.

3.1.7 réglementation technique [b-OMC-OTC]: document établissant les caractéristiques d'un produit ou les procédures et méthodes associées, y compris les dispositions administratives applicables, avec lesquelles la conformité est obligatoire. Il peut aussi porter, en partie ou en totalité, sur les exigences relatives à la terminologie, aux symboles, à l'emballage, au marquage et à l'étiquetage, dans la mesure où elles s'appliquent à un produit, une procédure ou une méthode de production.

3.1.8 marché gris [b-Gartner]: importation et vente de dispositifs en dehors des circuits de commercialisation ordinaires tels que définis par le fabricant ou les pouvoirs publics concernés, créant un marché en parallèle des circuits de distribution autorisés.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 dispositif TIC de contrefaçon: dispositif fondé sur les technologies de l'information et de la communication (TIC) qui enfreint expressément la marque de fabrique, copie les modèles de matériels et de logiciels, enfreint les droits liés à la marque ou à l'emballage d'un produit original ou authentique et, en règle générale, enfreint les normes techniques, les prescriptions règlementaires ou les procédures de conformité, les accords de licences de fabrication applicables aux niveaux national et/ou international ou les autres prescriptions juridiques applicables.

3.2.2 dispositif TIC altéré: dispositif fondé sur les technologies de l'information et de la communication (TIC) dont des composants, des logiciels, l'identificateur unique, des éléments protégés par des droits de propriété intellectuelle ou des marques de fabrique ont fait l'objet d'une tentative d'altération ou ont été effectivement altérés sans le consentement express du fabricant ou de son représentant légal.

3.2.3 identificateur unique: identificateur associé à un dispositif unique qui vise à l'identifier de manière univoque.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

ADPCI aspects des droits de propriété intellectuelle qui touchent au commerce

CAS système d'évaluation de la conformité (*conformity assessment scheme*)

DevID identificateur de dispositif (*device identifier*)

DIRBS système d'identification, d'enregistrement et de blocage des dispositifs (*device identification, registration, and blocking System*)

DPI droits de propriété intellectuelle

EAP protocole d'authentification extensible (*extensible authentication protocol*)

EIR registre d'identification des équipements (*equipment identity register*)

IMEI identité internationale d'équipement mobile (*international mobile equipment identity*)

IoT Internet des objets (*Internet of things*)

IVR réponse vocale interactive (*interactive voice response*)

OTC obstacle technique au commerce

PCB carte à circuit imprimé (*printed circuit board*)

SIM module d'identification de l'abonné (*subscriber identification module*)

TAC code d'attribution type (*type allocation code*)

TEE environnement d'exécution fiable (*trusted execution environment*)

TIC technologies de l'information et de la communication

TPM module de plate-forme fiable (*trusted platform module*)

5 Conventions

La présente Recommandation emploie les formes verbales ci-après lors de la formulation des dispositions:

a) L'expression "il est nécessaire" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité à la présente Recommandation.

b) Le terme "devait" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette exigence n'est donc pas indispensable pour déclarer la conformité.

c) Le terme "peut" indique une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Il ne doit pas être interprété comme l'obligation pour le fabricant de mettre en oeuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de service de l'activer ou non, mais comme la possibilité pour le fabricant de fournir ou non cette option, sans que cela n'ait d'incidence sur la déclaration de conformité à la présente Recommandation.

6 Aspects généraux

Ces dernières années, les dispositifs TIC sont de plus en plus utilisés et ont des répercussions positives dans la vie quotidienne, mais des effets secondaires indésirables liés à l'augmentation de la vente, de la circulation et de l'utilisation de dispositifs TIC de contrefaçon sur le marché ont aussi vu le jour. Cette situation engendre des conséquences négatives pour diverses parties prenantes, telles que les utilisateurs, les opérateurs de réseau, les fabricants de dispositifs authentiques, les négociants et les pouvoirs publics, notamment une diminution de la protection de la sécurité et de la qualité de service pour les utilisateurs, ainsi qu'un manque à gagner pour un éventail de parties prenantes.

Il est reconnu que le principe économique de l'offre et de la demande en ce qui concerne les dispositifs TIC de contrefaçon rend plus difficiles les initiatives prises pour lutter contre le marché noir et le marché gris à l'échelle mondiale et qu'aucune solution unique permettant de lutter contre la contrefaçon ne constitue une panacée. La présente Recommandation propose un cadre comportant une large gamme de mesures pouvant être prises et appliquées dans le cadre d'une approche globale pour faire face à ce problème. Il conviendrait aussi de lutter autant que possible contre la source des produits de contrefaçon sur les marchés où ils sont fabriqués et d'où ils sont exportés, avec le concours des pays dans lesquels ils sont vendus.

Il peut être particulièrement difficile pour toute personne réalisant l'inspection d'un dispositif TIC ou effectuant un essai sur celui-ci de déterminer s'il est authentique ou s'il s'agit d'un dispositif de contrefaçon, puisque l'objectif d'un contrefacteur est de créer des produits très ressemblants au dispositif original, en les accompagnant d'une fausse documentation ou d'une documentation volée, quelquefois en incluant du matériel ou des accessoires provenant du produit authentique et même en copiant le logiciel authentique ou les identificateurs uniques, tout ceci dans le but de rendre l'identification de ces produits difficile pour toutes les parties prenantes. Il est primordial de tenir compte de ces facteurs, entre autres, lors de la mise en oeuvre de solutions, afin d'éviter qu'elles ne

créent davantage de problèmes pour les utilisateurs et les fabricants de produits authentiques qu'elles ne permettent d'en résoudre.

Parmi les différents types de dispositifs TIC utilisés actuellement, les smartphones et autres dispositifs mobiles sont devenus des objets omniprésents et attrayants pour la population mondiale et, par voie de conséquence, ont également attiré l'attention du marché noir et du marché gris à l'échelle mondiale. En réponse au problème posé par les dispositifs TIC de contrefaçon, certains pays ont adopté des mesures et mis en place des solutions efficaces pour décourager la circulation et l'utilisation de ces dispositifs. Cependant, les pouvoirs publics d'autres pays sont mis à rude épreuve et sont incertains de la stratégie qu'il est préférable d'adopter.

Dans l'optique de s'attaquer au problème posé par l'utilisation de dispositifs TIC de contrefaçon, beaucoup de solutions mises en place ont certaines caractéristiques en commun, comme le fait d'être fondé sur des identificateurs de dispositifs uniques, l'appui d'un régime d'évaluation de la conformité ainsi que des moyens permettant d'empêcher les dispositifs frauduleux d'accéder au réseau (comme proposé pour les dispositifs mobiles dans l'Annexe A).

Toutefois, les pouvoirs publics de nombreux pays ont encore des difficultés à lutter contre la contrefaçon de dispositifs TIC pour différentes raisons, parmi lesquelles on peut citer des aspects techniques, les efforts fournis par les contrefacteurs pour que leurs produits échappent aux procédures de détection ainsi que le simple attrait de ces produits, incitant des consommateurs à prendre la décision d'acheter délibérément des produits de contrefaçon.

Par conséquent, les pays qui choisissent de lutter contre la contrefaçon des TIC devraient étudier les approches globales impliquant plusieurs organismes/parties prenantes ainsi que les solutions technologiques mises en oeuvre dans d'autres pays déjà engagés dans cette lutte, afin de tirer profit de leurs conseils et de leurs exemples en matière de bonnes pratiques.

7 Fondements d'un marché d'équipements de télécommunication sain

De nombreux facteurs sont à la base de la création d'un marché de produits et services de télécommunication sain. L'une des conditions fondamentales est l'établissement d'exigences techniques rigoureuses pour les produits qui entrent sur le marché. Ces exigences garantissent, entre autres, la sécurité des personnes, aussi bien la communauté d'utilisateurs que le personnel du fournisseur de services de réseau, ainsi que la mise en place d'un environnement sans brouillage pour les services de télécommunication.

L'absence de brouillage pour les services hertziens et filaires joue un rôle dans le développement économique d'une société, car la participation à l'économie numérique internationale nécessite que les plates-formes de télécommunication sur lesquelles ont lieu les activités économiques soient robustes, sécurisées et fiables. En outre, un marché dont le régime d'accès est bien défini, bien géré, non discriminatoire et transparent inspire la confiance des équipementiers, des fournisseurs de services et de la population en général. Un tel régime, appuyé par un cadre réglementaire et législatif adéquat, est un élément fondamental permettant d'assurer que la connectivité à l'échelle nationale et internationale présente la qualité requise, ce qui est essentiel pour participer à l'économie numérique internationale. En effet, le régime d'accès au marché rend compte de manière très fidèle des priorités et des valeurs d'une société [b-UIT-D-CI-Lignes directrices].

8 Aspects en prendre en considération lors de la mise en oeuvre de solutions pour lutter contre la contrefaçon de dispositifs TIC

Les parties prenantes doivent s'attaquer à plusieurs difficultés lors de la mise en oeuvre de solutions permettant de lutter contre la contrefaçon de dispositifs TIC:

8.1 Détection et identification des dispositifs TIC de contrefaçon

L'un des objectifs d'un contrefacteur est de faire en sorte que ses produits puissent être vendus sur les marchés du monde entier. De l'apparence au mode de fonctionnement, en passant par la copie des identificateurs uniques, des logiciels et même des composants internes des dispositifs TIC, les contrefacteurs vont faire de leur mieux pour que leur produit soit le plus ressemblant possible à l'original.

Cela présente quelques difficultés. Par exemple, tous les identifiants créés par les fabricants de produits authentiques peuvent faire et font l'objet d'une utilisation abusive par des contrefacteurs, qui cherchent à tromper les consommateurs et les autorités en leur faisant croire que le produit qu'ils proposent est authentique. Tous les mécanismes d'identification et les dispositifs de sécurité s'y rapportant sont susceptibles de devenir une cible pour les contrefacteurs et les délinquants. Les logos d'homologation et les icônes ainsi que les identifiants électroniques sont souvent détournés à dessein, voire ne sont pas définis en vue de leur auto-programmation sur les marchés locaux, afin d'éviter les contrôles douaniers et les vérifications effectuées par les services chargés de l'application de la loi aux frontières. [b-UIT-T TR-Contrefaçon]

Tous les identifiants créés par les fabricants de produits authentiques peuvent être falsifiés par des contrefacteurs, qui cherchent à tromper les consommateurs et les autorités en leur faisant croire que le produit qu'ils proposent est authentique. Ce problème se pose dans de nombreux secteurs, pas seulement dans celui des TIC. Il conviendrait de garder à l'esprit que les mécanismes d'identification et les dispositifs de sécurité qui s'y rapportent deviendront une cible pour les contrefacteurs et les délinquants. [b-UIT-T TR-Contrefaçon]

Par exemple, il est courant que les contrefacteurs falsifient les identificateurs uniques utilisés par certains dispositifs pour s'authentifier sur le réseau de sorte que les dispositifs TIC de contrefaçon soient reconnus par le réseau comme des équipements authentiques. Une autre pratique consiste à intercepter les dispositifs authentiques et à changer le logiciel qu'ils contiennent afin de les faire passer pour des versions plus récentes (et plus chères) ou encore à remplacer les éléments internes d'origine, tels que les batteries, par des modèles de contrefaçon, en vue de vendre les éléments d'origine sur le marché.

Les logos d'homologation et les icônes ainsi que les identifiants électroniques sont souvent détournés à dessein, afin d'éviter les contrôles douaniers et les vérifications effectuées par les services chargés de l'application de la loi aux frontières. Cette situation est source de problèmes pratiques pour les fabricants, les consommateurs, les autorités douanières et les agents des services chargés de l'application de la loi, qui rencontrent des difficultés pour distinguer les fausses marques d'identification des équipements de contrefaçon des marques authentiques, avant même le contrôle du produit concerné.

8.2 Repérage des fabricants et des trafiquants de dispositifs TIC de contrefaçon

Lorsqu'un dispositif illicite est identifié, les agents concernés devraient remonter jusqu'aux pays d'origine, fabricants et trafiquants des dispositifs illicites et exclure les fabricants et les trafiquants du marché [b-OCDE].

Sans une procédure d'identification des dispositifs de contrefaçon et des mesures coercitives à l'encontre des fabricants et trafiquants de ces produits efficaces dans les pays d'origine, les mesures prises dans les pays de destination risquent de ne pas être efficaces.

8.3 Élimination des dispositifs TIC de contrefaçon déjà utilisés sur le marché

Le contrôle des dispositifs TIC de contrefaçon après leur mise sur le marché dépend des mesures qu'il est possible de prendre à leur égard. Parmi les mesures envisageables, on peut citer i) la détection et la vérification de ces dispositifs, physiquement ou à distance, sur la base des caractéristiques du produit d'origine, ii) la suspension de leur utilisation ou iii) la saisie de ces articles.

Ces possibilités et ces mesures soulèvent plusieurs difficultés:

– Peu d'occasions permettent de vérifier physiquement un article: au cours d'une opération de réparation ou de surveillance du marché, ou dans une situation où une autorité juridique est habilitée à contrôler le dispositif. Dans ce cas, la difficulté réside dans la création de la base de connaissances requise ainsi que dans l'intérêt porté par les organismes concernés à la réalisation de ce genre de tâches.

– La vérification peut être effectuée de manière logique ou à distance, par exemple, en recoupant les identificateurs uniques et les empreintes du produit au cours d'un processus tel qu'un enregistrement en ligne. Cependant, cela nécessite généralement une connexion Internet, ce qui peut constituer une difficulté dans les environnements isolés ou ruraux, en particulier dans les pays en développement. Des procédures électroniques devraient être utilisées, mais il demeure indispensable de pouvoir confronter les caractéristiques physiques du produit avec les informations contenues dans les bases de données.

– Si l'enregistrement d'un dispositif sur le réseau se fait au moyen d'un identificateur unique, il est possible de refuser l'accès aux dispositifs TIC de contrefaçon à l'aide d'une base de données répertoriant les dispositifs dont le fonctionnement est autorisé sur un marché donné. La difficulté consiste à mettre en place le système d'enregistrement et la base de données ainsi qu'à en assurer la maintenance, en particulier dans le cas où de nombreux dispositifs ont déjà été déployés sans avoir été soumis à ce type de contrôle.

– Il conviendrait de veiller à éviter l'utilisation abusive des systèmes d'identification et d'enregistrement, à respecter les droits de consommateurs et à ne pas engendrer d'incidences négatives sur les utilisateurs de dispositifs TIC. Il conviendrait également de protéger les consommateurs contre toute déconnexion arbitraire des réseaux.

– La saisie de dispositifs TIC de contrefaçon est fondée sur une vérification physique et, dans la plupart des cas, elle supposera ou exigera l'intervention d'organismes chargés d'appliquer la loi en vertu d'un cadre juridique dans lequel s'inscrivent les éventuelles actions en justice. Les difficultés résident dans la mise en place d'une coopération entre les différents organismes, dans la définition d'un cadre juridique ainsi que dans la détermination des responsabilités relatives aux dispositifs TIC de contrefaçon.

– Les incidences sur l'utilisateur ne devraient pas être sous-estimées. Il conviendrait de tenir compte du fait que la déconnexion d'un dispositif puisse ne pas être autorisée dans certains pays et que l'utilisateur puisse être mis en danger de mort.

8.4 Limitation de l'importation, de la circulation et de la vente de nouveaux dispositifs TIC de contrefaçon sur le marché

Il conviendrait de prendre des mesures pour limiter l'importation, la contrebande, la circulation et la vente de nouveaux dispositifs TIC de contrefaçon sur le marché, en plus de celles visant à éliminer ceux qui sont stockés ou déjà utilisés.

Cette approche peut participer à la réduction de la présence globale des dispositifs TIC de contrefaçon sur le marché, compte tenu des contraintes financières et temporelles de l'administration ayant choisi de prendre ces mesures, et réduit les incidences sur l'utilisateur final, en comparaison avec des mesures consistant à déconnecter les dispositifs TIC de contrefaçon.

Comme indiqué au paragraphe 8.2, ces mesures devraient aussi porter sur les sources des dispositifs TIC de contrefaçon.

8.5 Distinction entre les dispositifs TIC authentiques et ceux de contrefaçon

Afin de garantir l'efficacité des mesures visant à éliminer les dispositifs TIC de contrefaçon déployés sur le marché et à empêcher que de nouveaux n'y pénètrent, il est nécessaire de mettre en place des solutions ainsi que de définir des critères permettant de distinguer les dispositifs authentiques de ceux de contrefaçon. Cette distinction doit être réalisée avec une grande exactitude, même lorsqu'il s'agit d'identificateurs uniques clonés, afin que des mesures disruptives puissent être prises, de préférence au moyen de systèmes automatisés, ou manuellement pour un nombre limité de dispositifs TIC.

Lorsque l'on cherche à effectuer une distinction entre les dispositifs TIC authentiques et ceux de contrefaçon, il conviendrait de tenir compte des points suivants:

– L'objectif du contrefacteur est de créer un produit très ressemblant au produit authentique d'origine.

– Le contrefacteur peut délibérément tenter de perturber l'inspection en joignant à ses produits de contrefaçon une documentation, un élément matériel ou un logiciel falsifiés ou bien authentiques mais dérobés.

– Certains éléments d'un produit de contrefaçon peuvent provenir d'un produit authentique et de ses accessoires, y compris notamment: les logiciels, les identificateurs uniques, les boîtiers, les cartes à circuit imprimé et les puces.

– Les micrologiciels et les logiciels des produits authentiques font l'objet de mises à jour régulières, principalement pour des raisons de sécurité. C'est également le cas des applications et de certains accessoires. Ainsi, il peut s'avérer difficile de définir une "empreinte" d'un dispositif authentique.

– Très souvent, une inspection visuelle ne suffira pas à déterminer l'authenticité d'un dispositif et une expertise technique plus poussée, des essais complémentaires ou des essais en laboratoire pourraient se révéler nécessaires.

8.6 Limitation des incidences sur les fabricants de dispositifs TIC authentiques

Les solutions mises en place pour lutter contre la contrefaçon de dispositifs TIC devraient avoir le moins d'incidences possible sur les fabricants de dispositifs TIC authentiques et porter principalement sur les dispositifs de contrefaçon ainsi que sur les fabricants et trafiquants de ces produits.

Par conséquent, les solutions qui engendrent des coûts supplémentaires pour les fabricants légitimes, lors de la fabrication ou de l'élimination des dispositifs authentiques, devraient être écartées, car elles servent aussi indirectement les intérêts des contrefacteurs, qui s'appuient généralement sur des prix bas pour inciter les consommateurs à choisir délibérément les dispositifs TIC de contrefaçon.

8.7 Réduction des incidences sur l'utilisateur final lorsque l'on envisage l'élimination des dispositifs TIC de contrefaçon

Lorsque la solution retenue consiste à éliminer ou à déconnecter les dispositifs TIC de contrefaçon, il conviendrait d'étudier soigneusement ses incidences sur l'utilisateur final et, lorsque plusieurs méthodes permettent d'atteindre le même objectif, il convient d'adopter celle qui limite le plus l'incidence globale sur le consommateur.

Il convient par conséquent de tenir compte des difficultés suivantes:

– Dans certains pays, il se peut que le fait de déconnecter des dispositifs TIC ne soit pas autorisé.

– Il n'est pas toujours possible de contacter les utilisateurs au moyen du dispositif considéré avant que ce dernier ne soit déconnecté (par exemple, dans le cas de dispositifs servant uniquement à l'envoi de SMS ou au transfert de données, du renvoi d'appel, de systèmes de réponse vocale interactive, etc., sans les coordonnées de l'utilisateur).

– Le blocage de dispositifs TIC de contrefaçon opérant dans des domaines sensibles (par exemple, les applications médicales, les services financiers, etc.) peut être délicat.
– Il convient de faire en sorte que les droits de l'utilisateur ne soient pas bafoués et que la mesure envisagée respecte la législation nationale.

8.8 Sensibilisation des consommateurs

Il conviendrait de sensibiliser les consommateurs sur les problèmes relatifs à l'achat et à l'utilisation continue de dispositifs TIC de contrefaçon, y compris les risques éventuels pour la santé et la qualité de service médiocre.

Il est nécessaire de prendre en compte le fait que les consommateurs choisissent souvent de manière délibérée d'acheter des biens de contrefaçon, en raison de leur prix, en dépit des conséquences éventuelles que cela peut avoir. Partant, il est essentiel de sensibiliser les consommateurs au sujet des incidences négatives liées à l'utilisation de dispositifs TIC de contrefaçon et des avantages que présentent les dispositifs authentiques.

8.9 Évitement des obstacles techniques au commerce

Il conviendrait d'être attentif à ne pas entraver l'importation et l'utilisation de dispositifs TIC authentiques, car cela constituerait un "obstacle technique au commerce (OTC)", tel que défini par l'Organisation mondiale du commerce (OMC) dans l'Accord sur les aspects des droits de propriété intellectuelle qui touchent au commerce (ADPIC) [b-Accord sur les ADPIC].

L'utilisation de "listes blanches" peut être concernée, car, par erreur ou en raison d'une mauvaise décision lors de la conception, cette solution pourrait empêcher des utilisateurs légitimes, y compris des voyageurs et des touristes, d'utiliser un dispositif TIC. Ce type d'exigences, relatives à l'enregistrement des dispositifs, pourraient malencontreusement constituer un OTC.

9 Exigences du cadre

Lors de la mise en place d'une solution visant à lutter contre la contrefaçon de dispositifs TIC, les pays doivent tenir compte des exigences suivantes:

9.1 Identification des dispositifs de contrefaçon et mesures coercitives à l'encontre des fabricants et trafiquants de ces dispositifs

Il est nécessaire d'établir une procédure, dans le cadre de la lutte contre l'utilisation de dispositifs TIC de contrefaçon déployés sur le marché ou qui entrent sur le territoire national, afin de remonter jusqu'à la source de ces produits et d'exclure du marché les fabricants et trafiquants à l'origine de leur déploiement.

Étant donné que les dispositifs TIC de contrefaçon traversent souvent plusieurs pays avant d'être vendus, il est nécessaire d'établir une collaboration étroite entre les parties prenantes impliquées dans cette procédure et leurs homologues dans les autres pays concernés, afin de répondre à cette exigence.

Il est demandé de pouvoir identifier les dispositifs de contrefaçon et de disposer de mesures coercitives à l'encontre des fabricants et des trafiquants de ces dispositifs dans les pays d'origine, comme indiqué au paragraphe 8.2.

9.2 Consultation du secteur privé et des associations de consommateurs

Il est nécessaire de consulter toutes les parties prenantes impliquées, notamment les opérateurs de réseau, le secteur privé et les associations de consommateurs, avant de prendre les mesures qui s'imposent, afin de pouvoir prendre connaissance des initiatives du secteur privé et de pouvoir parvenir à des accords concernant les mesures appropriées et raisonnables qu'il convient de prendre et qui auront le moins d'incidences sur les utilisateurs finals.

En outre, les consommateurs peuvent être sensibilisés au sujet de leurs devoirs et de leurs droits en matière d'utilisation et d'achat de dispositifs TIC. De plus, la lutte contre les dispositifs TIC de contrefaçon peut avoir une incidence négative réduite sur toutes les parties prenantes. Tous les efforts possibles devraient être déployés afin de réduire et éviter tout désagrément ou malentendu. Toutes les informations communiquées devraient être claires et faciles à comprendre pour les utilisateurs finals.

Il est aussi nécessaire de prendre des mesures axées sur la disponibilité et l'accessibilité des dispositifs et sur la sensibilisation des consommateurs au sujet des avantages liés à l'utilisation de dispositifs légaux et des aspects négatifs découlant de l'utilisation de produits de contrefaçon.

9.3 Identificateurs uniques fiables

Les dispositifs TIC authentiques doivent avoir des identificateurs uniques et permanents sécurisés, c'est-à-dire que ces identificateurs ne doivent pas pouvoir être modifiés par des entités non autorisées, qu'ils sont uniques pour chaque équipement et qu'ils ont été attribués par l'entité autorisée responsable de cette attribution.

Il est recommandé aux fabricants de placer cet identificateur unique sur un élément sécurisé de l'équipement et de mettre en oeuvre des mesures de sécurité, pour autant que cela soit techniquement réalisable, afin de détecter la falsification de l'identificateur unique et, le cas échéant, de rendre le dispositif inutilisable tant que l'identificateur d'origine n'est pas rétabli.

Il est recommandé à l'entité responsable de l'attribution des identificateurs de mettre en oeuvre une procédure garantissant que ces identificateurs uniques sont utilisés de manière adéquate et sécurisée.

9.4 Base de données centralisée de référence

Il est recommandé de mettre en place une base de données centralisée de référence répertoriant les équipements autorisés sur un marché particulier, à partir des identificateurs uniques, afin de différencier de manière efficace les dispositifs TIC authentiques de ceux de contrefaçon.

Lors de la conception de cette base de données, il conviendrait de tenir compte des points suivants:

– La base de données centralisée devrait être mise à la disposition des parties prenantes concernées du pays, telles que les autorités douanières, les services de police et les régulateurs, afin que ces institutions soient au fait des déplacements des marchandises et, le cas échéant, qu'elles puissent mettre fin à l'importation, la circulation et la vente de dispositifs TIC de contrefaçon entrant sur le marché et contribuer à l'identification des fabricants et trafiquants de produits de contrefaçon.

– La base de données centralisée devrait être l'élément central de la solution visant à éliminer les dispositifs TIC de contrefaçon déjà utilisés sur le marché.

– Il existe des bases de données pour certains marchés particuliers pouvant fournir des informations concernant les produits dans le pays concerné. Certaines d'entre elles sont des sous-ensembles d'une base de données mondiale ou sont liées d'une certaine manière à une base de ce type.

9.5 Mise en place d'un régime d'évaluation de la conformité

L'utilisation d'un système d'évaluation de la conformité (CAS) rigoureux déjà existant (ou la mise en place d'un tel système) est nécessaire pour mettre en oeuvre de manière efficace une base de données nationale centralisée de référence répertoriant les équipements autorisés, fondée sur les logos d'homologation, les icônes ou d'autres identificateurs uniques créés par des fabricants de produits authentiques, afin que toutes les parties prenantes (telles que les autorités douanières, les consommateurs et le secteur privé) puissent distinguer un dispositif TIC authentique d'un dispositif TIC de contrefaçon.

– Plusieurs administrations nationales, organisations régionales et internationales, entreprises privées ainsi que de nombreux acteurs du secteur des TIC ont mis en oeuvre des systèmes CAS efficaces. Conformément à la pratique générale, lorsque des dispositifs sont liés à l'utilisation des TIC à l'échelle mondiale, ils doivent nécessairement répondre à un ensemble de normes acceptées au niveau international et être soumis à des procédures d'évaluation de la conformité (par exemple, la procédure de l'UIT de reconnaissance des laboratoires – CASC, ISO/CASCO, CB de l'IECEE, GSMA, FCC, Innovation, Sciences et Développement économique Canada, ANATEL, GCF, PTCRB, ARIB, etc.).
– Ces organisations possèdent une grande quantité de données concernant le contrôle des produits, notamment les entités responsables de la fabrication et de la vente de ces produits; les ensembles de normes et de règlements nationaux (par exemple, l'attribution du spectre) et l'origine des produits.
– Il existe plusieurs façons de mettre en place un marché des TIC sain, par exemple, les différentes lignes directrices élaborées au titre du pilier 4 du programme C&I de l'UIT, que l'on trouvera sur le portail du programme C&I, disponible à l'adresse: https://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

9.6 Collaboration étroite avec les autorités douanières et les organismes locaux compétents

Afin de limiter efficacement la circulation, l'importation et la vente de nouveaux dispositifs TIC de contrefaçon sur le marché, il est nécessaire de mettre en place une collaboration étroite entre les autorités responsables de la base de données nationale centralisée de référence, les autorités douanières nationales ainsi que celles des autres pays concernés.

– Étant donné que les autorités douanières et les associations de consommateurs autorisées nationales compétentes jouent un rôle essentiel dans l'interception de produits de contrefaçon, il est important de mettre à leur disposition des outils permettant d'identifier les dispositifs TIC de contrefaçon, comme la base de données nationale centralisée de référence.
– Il est possible de lutter contre le commerce illégal de dispositifs TIC, y compris les dispositifs de contrefaçon, de contrebande et les dispositifs volés, au moyen de mécanismes d'authentification de l'identité d'un dispositif particulier, visant à vérifier que l'article est authentique, dans la mesure où les lois et les règlements du pays le permettent.
– Il convient d'établir et de mettre en oeuvre des mesures coercitives ainsi que d'instaurer et d'entretenir la communication entre les différentes organisations concernées, notamment en échangeant les informations pertinentes, telles que les bases de données nationales des dispositifs TIC conformes aux normes nationales, régionales ou internationales.
– Il est recommandé aux autorités douanières d'utiliser une plate-forme intergouvernementale en ligne permettant de partager des informations et des alertes au sujet des produits, de façon à faciliter l'identification des équipements de contrefaçon. On peut citer par exemple l'interface IPM de l'Organisation mondiale des douanes [b-OMD-IPM].

9.7 Partage des informations avec les utilisateurs finals avant de prendre des mesures correctives

Il est nécessaire d'informer les consommateurs des dangers relatifs à l'achat de dispositifs TIC de contrefaçon ainsi que du fait que l'utilisation de produits de contrefaçon n'est pas sans risque, ces produits ne fonctionnant peut-être pas aussi bien que des produits authentiques.

De plus, les raisons pour lesquelles les dispositifs TIC de contrefaçon ne sont pas autorisés (risques pour la sécurité, qualité de service médiocre et augmentation en conséquence du nombre de réclamations, risques de brouillages, atteintes aux droits de propriété intellectuelle, etc.) doivent être clairement expliquées aux consommateurs et tout renseignement erroné éventuel concernant les justifications des procédures ayant des incidences sur le marché devrait être clarifié.

Dans le cas où des solutions techniques sont mises au point en vue d'identifier les dispositifs TIC de contrefaçon, il est recommandé de mettre à la disposition du grand public un outil permettant de vérifier l'authenticité d'un produit.

9.8 Appui des cadres réglementaires et juridiques nationaux applicables

Avant de mettre en oeuvre des mesures restrictives à l'encontre des dispositifs TIC de contrefaçon, il est nécessaire de s'assurer du soutien du cadre réglementaire et juridique national applicable, notamment en ce qui concerne:

– la restriction de l'activation de dispositifs TIC de contrefaçon sur les réseaux de télécommunication;
– la restriction de l'importation, de la circulation et de la vente sur le marché des dispositifs TIC et accessoires de contrefaçon qui ne sont pas conformes au cadre juridique et réglementaire d'un pays;
– la mise au point des solutions nécessaires en vue de permettre aux autorités, aux consommateurs et aux acteurs des circuits de vente de distinguer les produits authentiques des produits de contrefaçon;
– l'amélioration des mesures de sécurité visant à décourager la fabrication de produits de contrefaçon et d'autres produits illicites;
– la mise en place d'un cadre juridique contre la falsification d'identificateurs uniques.

Lorsque cette exigence est prise en compte, il conviendrait de faire dûment référence à la législation et aux cadres réglementaires nationaux existants qui portent éventuellement sur les aspects considérés.

9.9 Prise en compte des produits déjà utilisés sur le marché

En amont de toute mesure disruptive sur les dispositifs TIC de contrefaçon présents sur le marché, il est recommandé de tenir compte de la nécessité de protéger les utilisateurs de ces produits. Cela devrait limiter les incidences négatives sur les utilisateurs de ces dispositifs, qui ne connaissent pas les dispositions nationales légales ou réglementaires, ou les exigences relatives à l'achat et à l'utilisation des dispositifs TIC de contrefaçon.

Le blocage de dispositifs TIC en service peut avoir des conséquences lourdes et inattendues sur les différents types de réseaux, les utilisateurs finals et les infrastructures. Dans ce cas, l'une des options possibles est d'adopter des mécanismes transitoires, en ne bloquant par exemple dans un premier temps que les nouveaux terminaux et en autorisant les dispositifs en service sur le réseau à continuer de fonctionner, à charge pour les utilisateurs de passer à terme à l'utilisation de terminaux authentiques.

10 Approches possibles en matière de solutions permettant de lutter contre la contrefaçon des TIC

Compte tenu des exigences formulées plus haut et des informations provenant des études de cas décrites dans [b-UIT-T TR-Contrefaçon] ou provenant d'autres sources, on trouvera dans ce qui suit la description de certaines approches possibles permettant de lutter contre la contrefaçon de dispositifs TIC ainsi que des considérations dont il conviendrait de tenir compte lors de la mise en place de certaines de ces solutions:

10.1 Interdiction de l'utilisation d'identificateurs invalides ou correspondant à des dispositifs qui ne sont pas authentiques

Si l'enregistrement d'un dispositif sur le réseau se fait au moyen d'un identificateur unique, il est possible de rejeter cet accès aux dispositifs TIC de contrefaçon en utilisant des bases de données répertoriant les dispositifs dont le fonctionnement est autorisé sur un marché particulier.

Dans ce cas, si le dispositif TIC est effectivement pourvu d'un identificateur unique fiable, il est possible de mettre en oeuvre des solutions consistant à:

– bloquer les équipements présentant un identificateur unique invalide sur les réseaux;

– bloquer l'utilisation des équipements non homologués par le régulateur;

– bloquer l'importation et la vente illégales de ces dispositifs.

Si cette approche est choisie, il est aussi recommandé de sensibiliser les consommateurs au sujet de ces exigences. De plus, il peut être nécessaire d'opérer des réformes de la législation à l'échelle nationale, comme indiqué au paragraphe 9.8.

Lorsque la solution adoptée pour lutter contre la contrefaçon de dispositifs TIC consiste à identifier et à bloquer les dispositifs dont l'identificateur unique est invalide, elle peut aussi contribuer à:

– garantir que seuls des dispositifs légaux sont importés ou vendus, ce qui a une incidence positive sur le paiement des droits de douane et de la taxe sur la valeur ajoutée;

– lutter contre le vol de dispositifs grâce à l'enregistrement de l'identificateur unique de l'équipement dérobé sur une "liste noire" suite à une demande légitime;

– garantir la protection des consommateurs contre l'utilisation d'équipements de mauvaise qualité, susceptibles de ne pas être autorisés ou de présenter un danger pour la santé, ou ne garantissant pas une qualité de service satisfaisante (cette protection est assurée par la mise en oeuvre d'un outil permettant de vérifier simplement l'authenticité d'un équipement avant son achat).

Lors du processus de normalisation, il convient de veiller au respect de la protection des informations personnelles et de faire en sorte que les mécanismes d'enregistrement des identificateurs n'aient pas d'incidences négatives pour les utilisateurs de dispositifs TIC. Il conviendrait également de protéger les consommateurs contre toute déconnexion arbitraire des réseaux.

L'Annexe A contient de plus amples informations concernant la mise en oeuvre éventuelle d'une solution axée sur les dispositifs mobiles.

10.2 Certification des dispositifs TIC et surveillance du marché

Comme indiqué au paragraphe 9.5, la mise en place d'un système d'évaluation de la conformité (CAS) peut participer à la création d'une base de données nationale de référence des équipements autorisés, contenant la liste des identificateurs uniques ainsi que des informations complémentaires concernant les dispositifs (par exemple, les marques de certification, les spécifications techniques et les caractéristiques physiques), afin que toutes les parties prenantes (telles que les autorités douanières, les consommateurs et le secteur privé) puissent identifier les dispositifs certifiés.

De plus, à l'aide de ces informations, les agents des douanes pourraient être à même d'identifier les produits de contrefaçon grâce à la mise en oeuvre de mécanismes de surveillance du marché et d'autres mesures coercitives pouvant s'avérer nécessaires. En outre, les importateurs ayant la réputation de ne pas respecter les contrôles à l'importation peuvent être identifiés et inscrits sur une liste spéciale. Lorsque des envois de dispositifs TIC sont importés par des contrebandiers, les autorités réglementaires peuvent être averties, afin qu'une décision de procéder à des inspections puisse être prise et que des mesures coercitives puissent être mises en oeuvre.

En tant que partie intégrante de la politique relative au système CAS, la surveillance du marché des équipements de télécommunication déployés a pour objectif de garantir que les produits mis sur le marché n'occasionnent pas de brouillages électromagnétiques, n'endommagent pas le réseau public de télécommunication et ne portent pas atteinte à la santé, à la sécurité ou à tout autre aspect relatif à la protection de la population.

Dans la pratique, la surveillance du marché implique de prendre les mesures requises (notamment des interdictions, des retraits ou des rappels) afin d'interrompre la circulation de produits qui ne sont pas conformes à toutes les exigences définies dans la législation et la réglementation pertinentes, de mettre les produits en conformité et d'appliquer des sanctions.

La surveillance du marché est essentielle pour le bon fonctionnement du marché des télécommunications, notamment pour assurer la protection des consommateurs et des employés contre les risques que comportent les produits non conformes. De plus, la surveillance du marché contribue à protéger les entreprises responsables face à la concurrence déloyale d'opérateurs économiques peu scrupuleux qui outrepassent ou contournent les règles.

De nombreux organismes de réglementation dans le monde sont soumis à des prescriptions juridiques particulières en ce qui concerne l'organisation de la surveillance du marché. En général, la règlementation fixe des obligations claires pour les autorités chargées de la surveillance du marché, spécifiant que ces autorités doivent avoir les pouvoirs, les ressources et les connaissances nécessaires pour remplir comme il se doit leurs fonctions [b-UIT-T-Portail-CI]. La règlementation exige la mise en place de procédures pour assurer le suivi des plaintes, la gestion des accidents ainsi que pour vérifier que les mesures correctives ont été prises et pour rassembler des connaissances scientifiques et techniques au sujet des questions de sécurité. En outre, les États Membres de l'UIT établissent, mettent en oeuvre et mettent régulièrement à jour les programmes nationaux de surveillance du marché; ils étudient et évaluent régulièrement le fonctionnement de leurs activités de surveillance, par exemple, à intervalles de quelques années. [b-UIT-D-CI-Lignes directrices]

Dans le Règlement (CE) N° 765/2008, la surveillance du marché est définie ainsi: opérations effectuées et mesures prises par des autorités désignées pour garantir que les produits sont conformes aux exigences légales définies dans la législation pertinente et ne portent pas atteinte à la santé et à la sécurité ou à tout autre aspect de la protection de l'intérêt public. [b-Règlement-CE]

Par conséquent, afin de compléter les mesures prises au moment où le produit atteint la frontière du pays, il est recommandé de réaliser des activités de surveillance supplémentaires visant les produits après leur entrée sur le marché pour contribuer à l'identification des biens de contrefaçon et, ainsi, garantir que le produit vendu à l'utilisateur final correspond à celui qui a été soumis au processus de certification. [b-Rapport-UIT-D]

La Commission économique pour l'Europe de l'Organisation des Nations Unies (CEE-ONU) recommande que les autorités nationales de surveillance du marché et les autorités douanières collaborent et que les détenteurs de droits aient la possibilité de fournir des informations aux autorités de surveillance du marché en ce qui concerne des marchandises de contrefaçon. [b-CEE-ONU]

10.3 Gestion du cycle de vie des dispositifs

Il est souhaitable de pouvoir distinguer un dispositif TIC original d'un clone, sans compromettre les droits des utilisateurs. En principe, les clones utilisent de manière abusive les identificateurs ou d'autres éléments d'identification uniques pour prétendre être le dispositif original.

Afin d'aider les parties prenantes et garantir l'authenticité des produits, l'une des solutions possibles devrait consister à mettre en place un système de gestion du cycle de vie des dispositifs, fondé sur les identificateurs uniques et capable d'assurer le suivi des dispositifs TIC depuis le début de leur fabrication (y compris l'origine des composants, le transport et le magasin où ils seront vendus) jusqu'à ce qu'ils soient cédés à l'utilisateur final.

Ces informations devraient être mises à la disposition de toutes les parties prenantes et, bien que les produits de contrefaçon puissent comporter des identificateurs uniques clonés, les autorités ainsi que les utilisateurs finals seraient en mesure de vérifier l'authenticité de ces informations. Par exemple, si un utilisateur se trouve dans un magasin, dans un certain pays et qu'en vérifiant l'identificateur unique, l'outil lui indique que ce produit est supposé être vendu dans un autre magasin, ou même dans un autre pays, cela indique de manière relativement claire que, même si l'identificateur est valide, le produit en question est une contrefaçon.

Il conviendrait d'être particulièrement attentif lors de l'utilisation de ce type de solution en ce qui concerne la revente des produits d'occasion par les utilisateurs finals, dans la mesure où la législation nationale devrait tenir compte de l'incidence de la gestion du lien entre l'utilisateur et le dispositif en matière de protection des informations personnelles.

Il conviendrait de tenir compte du fait que le produit identifié par ce type de méthode puisse ne pas être une contrefaçon, mais un produit authentique vendu sur le marché gris. Dans ce cas, des mesures supplémentaires pourraient être nécessaires pour identifier les produits de contrefaçon.

11 Cadre de référence

Compte tenu des points communs des différentes approches possibles abordées dans la section 10, la Figure 1 décrit une proposition de cadre permettant d'aborder les aspects liés à la production, à la circulation et à l'utilisation des dispositifs TIC de contrefaçon:

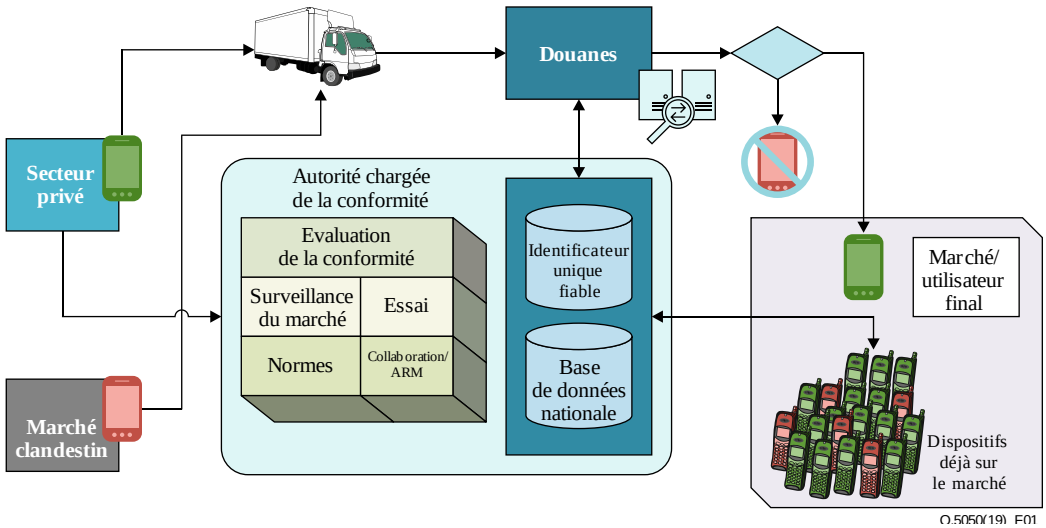

Figure 1 – Proposition de cadre général

Toute une gamme d'activités et de systèmes d'information, opérés par différentes organisations, doivent fonctionner en collaboration pour permettre le contrôle et la production d'informations essentielles visant à identifier les dispositifs altérés ou de contrefaçon et à lutter contre leur utilisation.

Dans le cadre des pratiques légales du commerce, lorsqu'un produit entre sur le territoire d'un pays, il est possible de vérifier sa conformité et de contrôler l'existence d'un représentant/responsable pour l'équipement concerné.

Lorsque les produits arrivent au niveau d'un point de contrôle, une entité (par exemple, les autorités douanières) vérifie tous les aspects juridiques des dispositifs, y compris leur conformité avec les exigences réglementaires et les conditions en matière d'obtention de certificats pertinentes, telles que les attributions de fréquences radioélectriques, la sécurité, l'interopérabilité, etc. Des contrôles

peuvent aussi être effectués pour vérifier que les dispositifs figurent sur liste blanche[1], afin de s'assurer que les identificateurs des dispositifs importés ont été attribués de façon légitime et que le contenu et le modèle du dispositif examiné correspondent aux détails enregistrés lors de l'attribution des identificateurs.

Lors de ce contrôle, les produits non autorisés, tels que les produits de contrefaçon, se voient refuser l'accès au marché. Le personnel de l'entité en question est appuyé par un régime d'évaluation de la conformité éventuellement en place et par une base de données contenant des renseignements au sujet des marchandises censées se trouver dans les conteneurs importés.

Ces bases de données de type inventaire peuvent aussi appuyer les mesures coercitives lorsque l'équipement (légal ou non) se trouve déjà sur le marché.

[1] Par exemple, la base de données globale des codes TAC de la GSMA peut être utilisée pour élaborer une liste blanche des dispositifs conformes aux spécifications 3GPP.

Annexe A

Solutions pour le cas de dispositifs mobiles

(La présente Annexe fait partie intégrante de la Recommandation.)

En ce qui concerne les dispositifs mobiles conformes aux spécifications 3GPP, certaines solutions permettant d'identifier les terminaux mobiles authentiques et importés légalement reposent sur l'utilisation du système d'enregistrement des identités internationales d'équipement mobile (IMEI). Les solutions reposant sur l'utilisation de identités IMEI pour lutter contre la contrefaçon des dispositifs mobiles sont fondées sur:

– le blocage sur les réseaux des dispositifs mobiles dont le numéro IMEI n'est pas valide (par exemple, aucune identité IMEI, identité IMEI exclusivement constituée de zéros, format de la chaine de caractère non conforme, identités IMEI dupliquées, identités IMEI attribuées par des organismes non autorisés ou identité IMEI valide mais n'ayant pas encore été attribuée par l'organisation désignée)[2];

– d'autres mesures axées sur la sensibilisation des consommateurs, des mesures coercitives et des réformes apportées à la législation à l'échelle nationale.

Afin de bloquer l'utilisation de dispositifs mobiles de contrefaçon, il est possible de mettre en place un système fondé sur l'enregistrement de tous les codes IMEI valides (identificateurs conformes aux normes, attribués officiellement par une organisation désignée à des produits importés légalement et homologués) des dispositifs mobiles actifs sur les réseaux nationaux. L'enregistrement des identités IMEI des dispositifs mobiles garantit que ces dispositifs sont conformes aux réglementations nationales et, dans certains pays, qu'ils ont été importés légalement.

- **Bases de données de référence**

Les codes IMEI sont utilisés afin de créer une base de données constituée d'une "liste blanche", d'une "liste grise" et d'une "liste noire" dans lesquelles sont répartis les dispositifs. La "liste blanche" répertorie les dispositifs dont l'utilisation est autorisée dans le pays considéré (par exemple, ceux qui ont été importés ou fabriqués légalement dans ce pays), la "liste grise" répertorie les dispositifs dont le statut n'est pas confirmé (qui n'entrent ni dans la "liste blanche", ni dans la "liste noire") et la "liste noire" répertorie les dispositifs pour lesquels les services doivent être rejetés dans le réseau de télécommunication.

Une analyse préalable devrait être effectuée afin de déterminer les incidences que pourrait avoir la mise en place d'une "liste blanche", d'une "liste grise" et d'une "liste noire" sur les réseaux et les utilisateurs, étant donné que ce système pourrait entraver la circulation des dispositifs entre les pays et avoir une incidence sur les visiteurs et les opérateurs étrangers.

La "liste grise" et la "liste noire" sont générées automatiquement par le traitement des données provenant de la "liste blanche" et des données fournies par les opérateurs, les importateurs et les autorités douanières.

- **Coordination avec le réseau de l'opérateur**

Pour garantir l'interaction active avec le système d'enregistrement, les opérateurs de télécommunication doivent tenir à jour leurs registres d'identification des équipements et faire en sorte que ces registres et la base de données des codes IMEI fassent l'objet d'une synchronisation régulière (par exemple, de façon quotidienne) et d'un échange de données automatique.

---

[2] La base de données globale des codes TAC de la GSMA peut être utilisée pour confirmer les cas de falsification ou de duplication d'identités IMEI pour les dispositifs conformes aux spécifications 3GPP.

Lorsqu'un téléphone mobile se raccorde au réseau d'un opérateur et s'y enregistre pour la première fois, son code IMEI est transféré par l'opérateur mobile dans la base de données. Le système indique les codes IMEI qui ne figurent pas dans la "liste blanche", identifie les dispositifs mobiles de contrefaçon et enregistre les codes IMEI correspondants dans la "liste grise". Le propriétaire du terminal concerné est informé par SMS et doit attester l'origine légale de son terminal dans un délai fixé à compter de la date d'inscription dans la "liste grise".

Il conviendrait de garantir la fiabilité et la sécurité du système d'enregistrement et des processus associés. Un accès est généralement fourni aux autorités réglementaires et douanières, aux opérateurs de réseaux et au grand public, avec des niveaux de privilèges d'accès appropriés. Les utilisateurs devraient avoir accès à cette base de données afin de pouvoir vérifier si un dispositif mobile est autorisé à fonctionner dans un pays particulier (généralement, en envoyant un SMS ou au moyen d'une page web).

Il est important de noter que les SMS devraient être considérés comme un moyen non sécurisé de communiquer avec le consommateur et qu'ils pourraient être utilisés par les fraudeurs. Il peut donc être nécessaire de prendre des mesures supplémentaires à cet égard.

- **Détection des codes IMEI clonés**

Étant donné qu'il est possible de falsifier les identificateurs uniques de certains dispositifs et qu'il est probable que les trafiquants commencent à cloner les identités IMEI des dispositifs authentiques afin de contourner ce système, des mesures supplémentaires devraient être mises en oeuvre afin d'identifier les dispositifs frauduleux présentant des identités IMEI légitimes clonées et d'agir à leur encontre.

Une méthode possible est l'adoption d'une base de données contenant des informations complémentaires sur les produits, pouvant être utilisées pour vérifier que les autres caractéristiques du produit qui utilise ces identificateurs correspondent bien avec ce qui est enregistré. Ces outils peuvent être mis en place avec l'appui d'un régime d'évaluation de la conformité qui recueillerait ces informations lors des procédures de certification des dispositifs et les stockerait dans une base de données à laquelle toutes les parties prenantes pourraient accéder.

- **Autres considérations**

Par ailleurs, une solution pour lutter contre la contrefaçon de dispositifs mobiles consistant à identifier et à bloquer les mobiles dont l'identité IMEI est invalide ou falsifiée peut contribuer à:

– bloquer l'importation illégale de ces dispositifs et, par conséquent, garantir que les dispositifs mobiles ont été importés et vendus légalement, ce qui peut avoir une incidence positive sur le paiement des droits de douane et de la taxe sur la valeur ajoutée;

– lutter contre le vol d'appareils, en inscrivant les codes IMEI des terminaux volés dans la "liste noire" suite à une demande légitime, ce qui rend le vol de terminaux inutile (on peut appliquer la même procédure pour le verrouillage du terminal, à la demande des propriétaires de téléphones perdus);

– bloquer l'utilisation d'équipements n'étant pas homologués par le régulateur, ce qui garantit la protection des consommateurs contre l'utilisation de terminaux mobiles de mauvaise qualité, susceptibles de ne pas être autorisés ou de présenter un danger pour la santé, ou ne garantissant pas une qualité de service satisfaisante en matière de communication mobile (cette protection est assurée par la mise en oeuvre d'un outil permettant de vérifier simplement l'authenticité d'un téléphone mobile avant son achat).

Il est important que l'approche reste coordonnée à l'échelle nationale, étant donné que les dispositifs TIC de contrefaçon peuvent être présents sur plusieurs réseaux. Le processus de détection devrait être efficace du point de vue des mesures à prendre, afin d'éviter les incidences multiples sur les utilisateurs, les chevauchements d'activités ou les conflits entre les différents opérateurs mobiles.

En vue de mettre en oeuvre ces solutions, il conviendrait que les études suivantes soient réalisées et examinées par toutes les parties prenantes: première phase de diagnostic (détermination de l'ampleur du problème des identificateurs invalides, clonés, etc.), planification de la procédure de détection et de contrôle ainsi que des ressources nécessaires (financières, humaines et temporelles) et analyse des incidences, afin de réduire celles qui concernent les utilisateurs finals.

Il conviendrait aussi de tenir compte que, dans certains cas, de tels mécanismes peuvent causer des problèmes à des utilisateurs légitimes, notamment des voyageurs et des touristes. Par exemple:

– Si un utilisateur se rend à l'étranger et utilise une carte SIM (module d'identification de l'abonné) locale dans son dispositif, ce dernier risque de ne pas figurer dans la liste blanche, ce qui empêchera son fonctionnement.

– Un visiteur en itinérance qui continue d'utiliser son dispositif pendant plusieurs mois peut aussi être pénalisé, à tort, par une liste blanche locale après une certaine période d'activité.

– Un message d'enregistrement peut être envoyé à un visiteur étranger qui utilise une carte SIM locale. Toutefois, il se peut que ce visiteur ne parle pas la langue locale et qu'il ne puisse pas comprendre le message en question. Par conséquent, il ne répondra pas à la demande d'enregistrement et son dispositif sera mis sur liste noire. En conséquence, soit: i) le visiteur est déconnecté du réseau local; soit ii) le dispositif du visiteur, bien que légitime, est placé sur liste noire dans d'autres pays, en raison d'accords de partage.

Étant donné que ces mécanismes, s'ils sont mis en oeuvre de façon inadéquate, peuvent causer des problèmes, il conviendrait de prévoir les cas de figure problématiques lors de la mise au point de ces mécanismes. Enfin, cette fonctionnalité ne doit pas être utilisée pour déconnecter arbitrairement des utilisateurs des réseaux pour d'autres raisons.

Appendice I

Autres solutions provenant du secteur privé

(Cet Appendice ne fait pas partie intégrante de la présente Recommandation.)

Le secteur privé a déployé de nombreux efforts pour faire face au problème des équipements de contrefaçon et pour améliorer la fiabilité des équipements et des entreprises. Ces efforts, à l'initiative du secteur privé, visent à mettre au point des solutions facultatives permettant d'améliorer la sécurité de la chaine d'approvisionnement. Les équipements de contrefaçon constituent un aspect de ces efforts, mais ce n'est pas le seul. Le secteur privé doit aussi travailler avec les pouvoirs publics, plus particulièrement, les autorités chargées de l'application de la loi et les autorités douanières, afin que des mesures coercitives soient prises. Il est préférable de voir les résultats de ces efforts comme des outils auxquels les entreprises peuvent faire appel en fonction de leurs besoins et des circonstances particulières (par exemple, un produit, un marché, etc.).

Il convient de noter que les activités du secteur privé en matière de produits de contrefaçon couvrent une gamme de produits très large, avec des chaines d'approvisionnement et des besoins variés. Il s'agit d'un processus interactif complexe dans lequel interviennent de nombreux acteurs. En plus de ces activités externes, les entreprises mènent des recherches extrêmement délicates et confidentielles et mettent sur pied des méthodes permettant de lutter contre la contrefaçon.

On trouvera ci-dessous un aperçu non exhaustif de certains efforts visant à améliorer la sécurité des dispositifs et pouvant contribuer à entraver la contrefaçon.

- **Base de données IMEI de la GSMA**

L'identité IMEI est un nombre à 15 chiffres utilisé pour identifier un dispositif sur un réseau mobile. Le code d'attribution type (TAC) est constitué des huit premiers chiffres de l'identité IMEI et identifie un modèle spécifique.

La GSMA (Global System for Mobile communications Association) tient à jour une base de données mondiale qui contient des informations concernant les codes TAC particuliers assignés aux dispositifs conformes aux spécifications 3GPP. Cette base de données est connue sous le nom de base de données IMEI.

Cette base de données pourrait être utilisée des façons suivantes:

– L'identification des dispositifs TIC de contrefaçon peut être effectuée en collaboration avec le fabricant légitime, qui peut être identifié à l'aide de la liste de la base de données TAC de la GSMA.

– La base de données TAC de la GSMA peut être mise à la disposition des entités publiques, telles que les ministères, les régulateurs, les autorités douanières et les entités chargées de l'application de la loi, en tant que source d'informations concernant la provenance et les spécifications des dispositifs mobiles. Ces informations peuvent être utilisées afin d'identifier les anomalies et les fabricants de dispositifs ne pouvant attester l'authenticité de leurs produits.

– L'authenticité des dispositifs mobiles de certains fabricants et leur identité IMEI peuvent être vérifiées au moyen de la base de données TAC de la GSMA. Les autorités douanières et les entités chargées de l'application de la loi peuvent recourir au centre d'assistance de la GSMA pour vérifier le numéro de série du certificat TAC soumis par le fabricant. Il s'agit d'un second numéro de série associé à chaque code TAC. L'absence de concordance entre ces identificateurs dénote une certaine forme de falsification des identificateurs.

– Les régulateurs peuvent utiliser la base de données TAC de la GSMA pour vérifier que les dispositifs mobiles testés dans le cadre de l'évaluation de la conformité correspondent à la description du modèle figurant dans la base de données.

Base de données IMEI de la GSMA: https://imeidb.gsma.com/imei/index

Services de la GSMA relatifs aux codes IMEI: https://www.gsma.com/services/tac-allocation/the-imei-database/

- **Système d'identification, d'enregistrement et de blocage des dispositifs**

Le système d'identification, d'enregistrement et de blocage des dispositifs (DIRBS) est une plate-forme logicielle basée sur un serveur permettant de faire face au problème des dispositifs mobiles illicites, volés ou de contrefaçon dans un pays. La plate-forme logicielle DIRBS est disponible sous forme de logiciel libre afin d'aider, entre autres, les gouvernements et les régulateurs dans leurs efforts pour lutter contre l'utilisation abusive de dispositifs illicites, volés ou de contrefaçon sur les réseaux cellulaires. Cette plate-forme est conforme aux recommandations de l'Union internationale des télécommunications en ce qui concerne les dispositifs illicites et non homologués dans un pays.

Le système DIRBS consiste en une base de données des dispositifs à l'échelle nationale, interagissant suivant différents niveaux de détail avec les opérateurs, les fabricants locaux, les importateurs, les consommateurs, les autorités douanières, les autorités chargées de l'application de la loi et la base de données mondiale IMEI de la GSMA. La plate-forme DIRBS est constituée d'un moteur d'analyse ainsi que de sous-systèmes associés fournissant les informations permettant de bloquer les dispositifs de contrefaçon ou les dispositifs frauduleux; le blocage effectif est régi par des règles propres au pays et réalisé au moyen des mécanismes du registre d'identification des équipements de l'opérateur.

De plus amples informations sont disponibles à l'adresse: www.qualcomm.com/dirbs

- **Trusted Computing Group**

Le Trusted Computing Group (TCG) est une organisation à but non lucratif constituée pour élaborer, définir et promouvoir des normes industrielles mondiales ouvertes, ne privilégiant aucun fournisseur et favorables à la constitution d'une racine de confiance relative au matériel pour les plates-formes informatiques fiables interopérables.

Le TCG a notamment élaboré des spécifications relatives à un module de plate-forme fiable (TPM) qui se rapportent au sujet traité dans la présente Recommandation:

http://www.trustedcomputinggroup.org/resources/tpm_main_specification

http://www.trustedcomputinggroup.org/resources/trusted_platform_module_tpm_summary

Comme indiqué dans le site web ci-dessus, un module TPM est une puce informatique (microcontrôleur) pouvant stocker de manière sécurisée les éléments utilisés pour l'authentification de la plate-forme (votre PC ou ordinateur portable). Ces éléments peuvent comprendre des mots de passe, des certificats ou des clés de chiffrement.

Ce mécanisme permet de réaliser des attestations tant localement qu'à distance, ce qui contribue à instaurer la confiance quant à l'authenticité de l'équipement.

Le TCG a aussi mis en place un groupe de travail sur les systèmes intégrés afin de traiter la question de la sécurité de ces systèmes, y compris l'Internet des objets:

http://www.trustedcomputinggroup.org/developers/embedded_systems

- **Global Platform**

Global Platform a élaboré les normes relatives à l'environnement d'exécution fiable (TEE), qui constitue la méthode adoptée dans les dispositifs mobiles actuels pour stocker et exécuter de manière sécurisée le code et les ressources sensibles relatifs à la sécurité.

De plus amples informations sont disponibles à l'adresse:
https://www.globalplatform.org/specificationsdevice.asp.

- **ISO/CEI JTC1/SC27**

Le domaine de compétence du Comité d'étude 27 (SC27) est important pour les activités du secteur privé qui concernent la sécurité, la lutte contre la contrefaçon et l'élaboration de normes relatives à la protection de l'information et aux TIC. Les activités de ce comité portent notamment sur les méthodes génériques, les techniques et les lignes directrices visant à traiter les aspects de sécurité et de protection des informations personnelles.

Le SC27 a notamment publié des normes au sujet des équipements de contrefaçon, parmi lesquelles on trouve:

– [b-ISO/CEI 15408] *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI (Critères communs)*;

– [b-ISO/CEI 27034] *Technologies de l'information – Techniques de sécurité – Sécurité des applications*;

– [b-ISO/CEI 27036-3] *Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur – Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information*;

– [b-ISO/CEI 20243] *Technologies de l'information – Norme de fournisseur de technologie de confiance ouverte (O-TTPS) – Atténuation des produits contrefaits et malicieusement contaminés*.

De plus amples informations sont disponibles à l'adresse: http://www.din.de/en/meta/jtc1sc27.

- **The Open Group Trusted Technology Forum**

The Open Group Trusted Technology Forum (OTTF) dirige l'élaboration d'un programme et d'un cadre à l'échelle mondiale relatifs à l'intégrité de la chaîne d'approvisionnement, visant à fournir aux acheteurs de produits informatiques un choix de partenaires et de vendeurs utilisant des technologies agréées. Il convient de noter que la norme [b-ISO/CEI 20243] mentionnée plus haut avait préalablement été mise au point par The Open Group.

De plus amples informations sont disponibles à l'adresse:
http://www.opengroup.org/getinvolved/forums/trusted.

- **Institute of Electrical and Electronics Engineers**

L'Institute of Electrical and Electronics Engineers (IEEE) a élaboré une norme relative à l'identité sécurisée des dispositifs et une méthode pour lier cryptographiquement l'identité et le dispositif, notamment IEEE 802.1ar: "Norme pour les réseaux locaux ou métropolitains: Identité sécurisée des dispositifs".

Comme indiqué sur le site web de l'IEEE, cette norme définit les identificateurs sécurisés des dispositifs (DevIDs), conçus pour être utilisés en tant que certificats d'authentification sécurisés des dispositifs interopérables dans le cadre du protocole d'authentification extensible ainsi que d'autres protocoles normalisés d'authentification et de mise en service utilisés dans le secteur privé. Une identité de dispositif normalisée facilite l'authentification sécurisée des dispositifs interopérables et simplifie le déploiement et la gestion sécurisés des dispositifs.

De plus amples informations sont disponibles à l'adresse:
http://www.ieee802.org/1/pages/802.1ar.html.

- **Exemples d'autres activités du secteur privé relatives à la contrefaçon**

ICC – Bureau d'enquêtes sur la contrefaçon

http://www.iccwbo.org/products-and-services/fighting-commercial-crime/counterfeiting-intelligence-bureau/

ICC – Plan d'action des entreprises pour mettre un terme à la contrefaçon et au piratage (BASCAP)

http://www.iccwbo.org/Advocacy-Codes-and-Rules/BASCAP/Welcome-to-BASCAP/

Bibliographie

[b-UIT-T-Portail-CI] Sous "Pilier 4", le portail de l'UIT sur la conformité et l'interopérabilité contient des informations à jour concernant le cadre réglementaire des pays en matière de conformité et d'interopérabilité http://www.itu.int/en/ITU-T/C-I/Pages/default.aspx.

[b-UIT-T TR-Contrefaçon] Rapport technique sur la contrefaçon de dispositifs TIC (2015).

[b-IEEE 802.1] IEEE 802.1 (2009), *Standard for Local and Metropolitan Area Networks: Secure Device Identity.* – http://www.ieee802.org/1/pages/802.1ar.html.

[b-ISO/CEI 15408-1] ISO/CEI 15408-1:2009, *Technologies de l'information – Techniques de sécurité – Critères d'évaluation pour la sécurité TI – Partie 1: Introduction et modèle général*.

[b-ISO/CEI 17000] ISO/CEI 17000:2004, *Évaluation de la conformité – Vocabulaire et principes généraux*.

[b-ISO/CEI 20243] ISO/CEI 20243:2015, *Technologies de l'information – Norme de fournisseur de technologie de confiance ouverte (O-TTPS) – Atténuation des produits contrefaits et malicieusement contaminés*.

[b-ISO/CEI 27034] ISO/CEI 27034:2011, *Technologies de l'information – Techniques de sécurité – Sécurité des applications*.

[b-ISO/CEI 27036-3] ISO/CEI 27036-3:2013, *Technologies de l'information – Techniques de sécurité – Sécurité d'information pour la relation avec le fournisseur – Partie 3: Lignes directrices pour la sécurité de la chaîne de fourniture des technologies de la communication et de l'information*.

[b-Règlement-CE] Règlement (CE) N° 765/2008 concernant la surveillance du marché.

[b-Gartner] https://www.gartner.com/it-glossary/gray-market

[b-UIT-D-CI-Lignes directrices] Lignes directrices de l'UIT sur la mise en place de systèmes pour la conformité et l'interopérabilité: Lignes directrices complètes (2015), UIT http://www.itu.int/en/ITU-D/Technology/Documents/ConformanceInteroperability/publications/Establishing_Conformity_and_interoperability_Regimes-E.pdf.

[b-Rapport-UIT-D] Rapport final sur la Question 4/2 – Question 4/2: Assistance aux pays en développement concernant la mise en oeuvre de programmes de conformité et d'interopérabilité, Commissions d'études de l'UIT-D, 2017, https://www.itu.int/pub/D-STG-SG02.04.1-2017.

[b-OCDE] Rapport de 2017 de l'OCDE intitulé "Trade in Counterfeit ICT Goods".

[b-Accord sur les ADPIC] Aspects des droits de propriété intellectuelle qui touchent au commerce; annexe de l'Accord de Marrakech instituant l'Organisation mondiale du commerce, signé à Marrakech (Maroc), le 15 avril 1994.

[b-CEE-ONU] Recommandation M. intitulée "Utilisation de la surveillance des marchés comme moyen complémentaire de protéger les consommateurs des marchandises de contrefaçon" http://www.unece.org/fileadmin/DAM/trade/wp6/Recommendations/Rec_M.pdf.

[b-OMD-IPM] Interface IPM de l'Organisation mondiale des douanes – http://www.wcoipm.org/.

[b-OMC-OTC] Organisation mondiale du commerce (OMC) – Accord sur les obstacles techniques au commerce (OTC).

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes de tarification et de comptabilité et questions de politique générale et d'économie relatives aux télécommunications internationales/TIC
Série E	Exploitation générale du réseau, service téléphonique, exploitation des services et facteurs humains
Série F	Services de télécommunication non téléphoniques
Série G	Systèmes et supports de transmission, systèmes et réseaux numériques
Série H	Systèmes audiovisuels et multimédias
Série I	Réseau numérique à intégration de services
Série J	Réseaux câblés et transmission des signaux radiophoniques, télévisuels et autres signaux multimédias
Série K	Protection contre les perturbations
Série L	Environnement et TIC, changement climatique, déchets d'équipements électriques et électroniques, efficacité énergétique; construction, installation et protection des câbles et autres éléments des installations extérieures
Série M	Gestion des télécommunications y compris le RGT et maintenance des réseaux
Série N	Maintenance: circuits internationaux de transmission radiophonique et télévisuelle
Série O	Spécifications des appareils de mesure
Série P	Qualité de transmission téléphonique, installations téléphoniques et réseaux locaux
Série Q	**Commutation et signalisation et mesures et tests associés**
Série R	Transmission télégraphique
Série S	Equipements terminaux de télégraphie
Série T	Terminaux des services télématiques
Série U	Commutation télégraphique
Série V	Communications de données sur le réseau téléphonique
Série X	Réseaux de données, communication entre systèmes ouverts et sécurité
Série Y	Infrastructure mondiale de l'information, protocole Internet, réseaux de prochaine génération, Internet des objets et villes intelligentes
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication

Imprimé en Suisse
Genève, 2019