Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

X.1368

(01/2021)

SÉRIE X: RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

Applications et services sécurisés (2) – Sécurité de l'Internet des objets (IoT)

Mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets

Recommandation UIT-T X.1368

RECOMMANDATIONS UIT-T DE LA SÉRIE X

RÉSEAUX DE DONNÉES, COMMUNICATION ENTRE SYSTÈMES OUVERTS ET SÉCURITÉ

RÉSEAUX PUBLICS DE DONNÉES	X.1–X.199
INTERCONNEXION DES SYSTÈMES OUVERTS	X.200–X.299
INTERFONCTIONNEMENT DES RÉSEAUX	X.300–X.399
SYSTÈMES DE MESSAGERIE	X.400–X.499
ANNUAIRE	X.500–X.599
RÉSEAUTAGE OSI ET ASPECTS SYSTÈMES	X.600–X.699
GESTION OSI	X.700–X.799
SÉCURITÉ	X.800–X.849
APPLICATIONS OSI	X.850–X.899
TRAITEMENT RÉPARTI OUVERT	X.900–X.999
SÉCURITÉ DE L'INFORMATION ET DES RÉSEAUX	
Aspects généraux de la sécurité	X.1000–X.1029
Sécurité des réseaux	X.1030–X.1049
Gestion de la sécurité	X.1050–X.1069
Télébiométrie	X.1080–X.1099
APPLICATIONS ET SERVICES SÉCURISÉS (1)	
Sécurité en multidiffusion	X.1100–X.1109
Sécurité des réseaux domestiques	X.1110–X.1119
Sécurité des télécommunications mobiles	X.1120–X.1139
Sécurité de la toile	X.1140–X.1149
Protocoles de sécurité (1)	X.1150–X.1159
Sécurité d'homologue à homologue	X.1160–X.1169
Sécurité des identificateurs en réseau	X.1170–X.1179
Sécurité de la télévision par réseau IP	X.1180–X.1199
SÉCURITÉ DU CYBERESPACE	
Cybersécurité	X.1200–X.1229
Lutte contre le spam	X.1230–X.1249
Gestion des identités	X.1250–X.1279
APPLICATIONS ET SERVICES SÉCURISÉS (2)	
Communications d'urgence	X.1300–X.1309
Sécurité des réseaux de capteurs ubiquitaires	X.1310–X.1319
Sécurité des réseaux électriques intelligents	X.1330–X.1339
Courrier certifié	X.1340–X.1349
Sécurité de l'Internet des objets (IoT)	**X.1360–X.1369**
Sécurité des systèmes de transport intelligents	X.1370–X.1389
Sécurité de la technologie des registres distribués	X.1400–X.1449
Protocoles de sécurité (2)	X.1450–X.1459
ÉCHANGE D'INFORMATIONS SUR LA CYBERSÉCURITÉ	
Aperçu général de la cybersécurité	X.1500–X.1519
Échange concernant les vulnérabilités/les états	X.1520–X.1539
Échange concernant les événements/les incidents/l'heuristique	X.1540–X.1549
Échange de politiques	X.1550–X.1559
Heuristique et demande d'informations	X.1560–X.1569
Identification et découverte	X.1570–X.1579
Échange garanti	X.1580–X.1589
SÉCURITÉ DE L'INFORMATIQUE EN NUAGE	
Aperçu de la sécurité de l'informatique en nuage	X.1600–X.1601
Conception de la sécurité de l'informatique en nuage	X.1602–X.1639
Bonnes pratiques et lignes directrices concernant la sécurité de l'informatique en nuage	X.1640–X.1659
Mise en œuvre de la sécurité de l'informatique en nuage	X.1660–X.1679
Sécurité de l'informatique en nuage (autres)	X.1680–X.1699
COMMUNICATIONS QUANTIQUES	
Terminologie	X.1700–X.1701
Générateur quantique de nombres aléatoires	X.1702–X.1709
Cadre de sécurité pour les réseaux QKDN	X.1710–X.1711
Conception de la sécurité pour les réseaux QKDN	X.1712–X.1719
Techniques de sécurité pour les réseaux QKDN	X.1720–X.1729
SÉCURITÉ DES DONNÉES	
Sécurité des mégadonnées	X.1750–X.1759
SÉCURITÉ DE LA 5G	X.1800–X.1819

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

Recommandation UIT-T X.1368

Mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets

Résumé

La Recommandation UIT-T X.1368 définit: 1) des modèles et procédures de base pour la mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets (IoT); et 2) les exigences et les capacités relatives à la mise à jour des micrologiciels de l'IoT.

Une procédure de mise à jour sécurisée commune, assortie d'exigences générales, est décrite. Cette procédure permet de mettre en œuvre de manière sécurisée les mises à jour communes des logiciels/micrologiciels de l'IoT entre les parties prenantes de l'environnement IoT, telles que les concepteurs de dispositifs IoT et les fournisseurs de systèmes/services IoT.

Cette Recommandation porte principalement sur la mise à jour des micrologiciels, mais s'applique aussi à la mise à jour de tout autre logiciel des dispositifs IoT.

Historique

Edition	Recommandation	Approbation	Commission d'études	Identifiant unique*
1.0	UIT-T X.1368	07-01-2021	17	11.1002/1000/14445

Mots clés

Mise à jour des logiciels, IoT, sécurité.

* 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 ou par des droits d'auteur afférents à des logiciels, et dont l'acquisition pourrait être requise 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 responsables de la mise en œuvre de consulter les bases de données appropriées de l'UIT-T disponibles sur le site web de l'UIT-T à l'adresse http://www.itu.int/ITU-T/ipr/.

Table des matières

Introduction

Les cyberattaques contre les dispositifs ou les systèmes de l'Internet des objets (IoT) deviennent de plus en plus ingénieuses, intelligentes et variées. Auparavant, les fonctions de la plupart des dispositifs IoT étaient déterminées par les fournisseurs de dispositifs IoT lors de la phase de diffusion initiale de ces dispositifs. Toutefois, depuis peu, les dispositifs sont connectés à l'Internet pour fournir un ensemble amélioré de services IoT. Par conséquent, les dispositifs IoT utilisés sont confrontés à des cybermenaces ou à des attaques. Il convient de reconnaître que les micrologiciels ou les logiciels mis en œuvre dans les dispositifs IoT doivent être mis à jour de manière sécurisée pour corriger leurs vulnérabilités et leurs faiblesses. Certains fournisseurs de dispositifs ont d'ores et déjà commencé à fournir un service de mise à jour des micrologiciels à l'aide de leurs propres systèmes.

On trouvera dans la présente Recommandation des modèles et des procédures de base concernant la mise à jour sécurisée des logiciels/micrologiciels de l'IoT, ainsi que les exigences et les capacités associées. Les modèles de base et la procédure de mise à jour commune permettent l'échange en toute sécurité des logiciels/micrologiciels de l'IoT entre les parties prenantes de l'environnement IoT, et visent à encourager ces dernières à mettre à jour les logiciels/micrologiciels de l'IoT devenus obsolètes.

Recommandation UIT-T X.1368

Mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs de l'Internet des objets

1 Domaine d'application

La présente Recommandation décrit des modèles et des procédures de base concernant la mise à jour sécurisée des micrologiciels ou des logiciels des dispositifs IoT. En outre, elle décrit les exigences et les capacités relatives à la mise à jour des micrologiciels/logiciels de l'IoT. La présente Recommandation porte principalement sur la mise à jour des micrologiciels, mais s'applique aussi à la mise à jour de tout autre logiciel des dispositifs IoT.

2 Références

Aucune.

3 Définitions

3.1 Termes définis ailleurs

Aucun.

3.2 Termes définis dans la présente Recommandation

La présente Recommandation définit les termes suivants:

3.2.1 auteur: entité qui produit des images de micrologiciel et des logiciels pour les dispositifs de l'Internet des objets. Il peut s'agir par exemple d'un individu ou d'un groupe, par exemple une entreprise ou tout autre type d'organisation. Un auteur peut télécharger l'image sur un ou plusieurs serveurs de micrologiciel qui ne sont pas nécessairement de confiance.

3.2.2 consommateur de micrologiciel: entité qui stocke, vérifie et exécute les images de micrologiciel sur un dispositif de l'Internet des objets. Le consommateur de micrologiciel devrait décider d'exécuter ou non les images de micrologiciel actuelles. Il existe un ou plusieurs consommateurs de micrologiciel pour un dispositif IoT.

3.2.3 serveur de micrologiciel: entité qui distribue des images de micrologiciel. Le serveur de micrologiciel pourrait accepter des images de micrologiciel provenant de plusieurs auteurs; il pourrait s'agir d'un répertoire pour tel ou tel fournisseur ou d'un répertoire qui accepte plusieurs fournisseurs. Théoriquement, un serveur de micrologiciel est fiable, mais il pourrait ne pas l'être; il pourrait essayer de visualiser ou de modifier les ensembles de micrologiciels reçus des auteurs.

3.2.4 manifeste: enregistrement qui contient les métadonnées d'une image de micrologiciel.

3.2.5 dispositif de suivi du statut: entité qui vérifie et suit de près le statut des images de micrologiciel à l'intérieur d'un ou de plusieurs consommateurs de micrologiciel et qui lance les mises à jour de micrologiciel nécessaires. Cela consiste à assurer un suivi précis des modifications au niveau du dispositif, par exemple la version des images de micrologiciel en cours d'exécution et l'état du cycle de mise à jour du micrologiciel dans lequel se trouve le dispositif. Un système de suivi du statut peut être installé à l'intérieur d'un dispositif de l'Internet des objets, sur l'Intranet ou l'Internet.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

DLT technologie des registres distribués (*distributed ledger technology*)

FW micrologiciel (*firmware*)

IoT Internet des objets (*internet of things*)

SW logiciel (*software*)

URL localisateur uniforme de ressource (*uniform resource locator*)

5 Conventions

La présente Recommandation suit les conventions ci-après, qui sont conformes à la publication [b-IETF RFC 2119]:

"doit" Ce mot signifie que la définition constitue une exigence absolue dans la présente spécification.

"ne doit pas" Cette expression signifie que la définition constitue une interdiction absolue dans la présente spécification.

"devrait" Ce mot signifie qu'il peut y avoir des raisons valables, dans des circonstances particulières, de ne pas tenir compte de l'énoncé considéré, mais il convient cependant de bien mesurer et examiner toutes les conséquences d'un tel choix avant de choisir une option différente.

"ne devrait pas" Cette forme verbale signifie qu'il peut exister des raisons valables dans des circonstances particulières, lorsque le comportement indiqué est acceptable ou même utile, mais il faut en comprendre toutes les conséquences et peser attentivement les choses avant de mettre en œuvre tout comportement décrit avec cette mention.

"peut" Ce mot signifie que l'énoncé considéré ne revêt qu'un caractère facultatif. Un fournisseur peut choisir de tenir compte de cet énoncé, par exemple parce que ce dernier correspond aux exigences d'un marché donné ou parce qu'il permet d'améliorer le produit proposé, alors qu'un autre fournisseur peut décider de ne pas tenir compte de ce même énoncé.

6 Modèle de base

L'architecture de réseau des dispositifs IoT peut varier, mais quatre entités fonctionnelles devraient être utilisées dans tous les cas, à savoir le consommateur de micrologiciel (voir le § 3.2.2), le dispositif de suivi du statut (voir le § 3.2.5), l'auteur (voir le § 3.2.1) et le serveur de micrologiciel (voir le § 3.2.3). Il convient de noter que plusieurs entités fonctionnelles peuvent se trouver à l'intérieur d'un même nœud. Ainsi, une webcam contient plusieurs consommateurs de micrologiciel et un dispositif de suivi du statut, tandis qu'un serveur web contient un dispositif de suivi du statut et un serveur de micrologiciel. Plusieurs consommateurs de micrologiciel peuvent se trouver dans un même réseau et sont surveillés par un dispositif de suivi du statut mis en place à l'intérieur de la passerelle. En fonction de l'importance des contraintes imposées aux dispositifs IoT, ces conceptions peuvent varier. Les modèles de déploiement types sont décrits au § 8.

Dans le modèle de base, ces entités jouent un rôle indispensable dans la mise à jour des logiciels/micrologiciels de l'IoT. Le scénario de base de ce modèle est simple: *un dispositif de suivi du statut qui reconnaît la nécessité d'une mise à jour des logiciels/micrologiciels de l'IoT lance la procédure de mise à jour des logiciels/micrologiciels qui permet aux consommateurs de micrologiciels de recevoir une image de logiciel/micrologiciel d'un auteur par l'intermédiaire d'un serveur de micrologiciel*.

7 Procédures de mise à jour

La Figure 1 illustre la procédure de base applicable à la mise à jour du micrologiciel. Avant de lancer la procédure de mise à jour du micrologiciel, un auteur doit télécharger une nouvelle image de micrologiciel sur un serveur de micrologiciel. Il est souhaitable que l'image soit accompagnée d'une signature numérique et soit chiffrée par l'auteur.

Lorsqu'un dispositif de suivi du statut reçoit la demande de mise à jour d'une image de micrologiciel avec son emplacement [par exemple, son localisateur uniforme de ressources (URL)], il vérifie la demande et vérifie ensuite, si la demande est valable, le statut du micrologiciel en communiquant avec le consommateur de micrologiciel, afin de confirmer la nécessité d'une mise à jour du micrologiciel. On trouvera au § 9 quelques moyens types permettant d'envoyer de telles demandes.

Si la nécessité de mettre à jour le micrologiciel est vérifiée, le consommateur de micrologiciel lance une mise à jour du micrologiciel, en communiquant l'emplacement du micrologiciel disponible. Le consommateur de micrologiciel demande ensuite au serveur de micrologiciel de lui fournir l'image à jour du micrologiciel. Le serveur de micrologiciel fournit l'image de micrologiciel au consommateur de micrologiciel, à condition que ce dernier ait le droit légitime de recevoir la mise à jour. Si tel n'est pas le cas, le serveur envoie un message de mise à jour avec un code d'erreur.

Lorsqu'il reçoit le message de mise à jour, le consommateur de micrologiciel vérifie l'image. Si aucune erreur n'est décelée, le consommateur de micrologiciel installe le micrologiciel et envoie des informations sur le statut de l'image au dispositif de suivi du statut. Il convient de noter que les cardinalités des quatre entités fonctionnelles ci-dessus sont de type "de plusieurs à plusieurs", c'est-à-dire que plusieurs dispositifs de suivi du statut peuvent communiquer avec plusieurs consommateurs de micrologiciel, qui peuvent à leur tour communiquer avec plusieurs serveurs de micrologiciel, qui peuvent communiquer avec plusieurs auteurs.

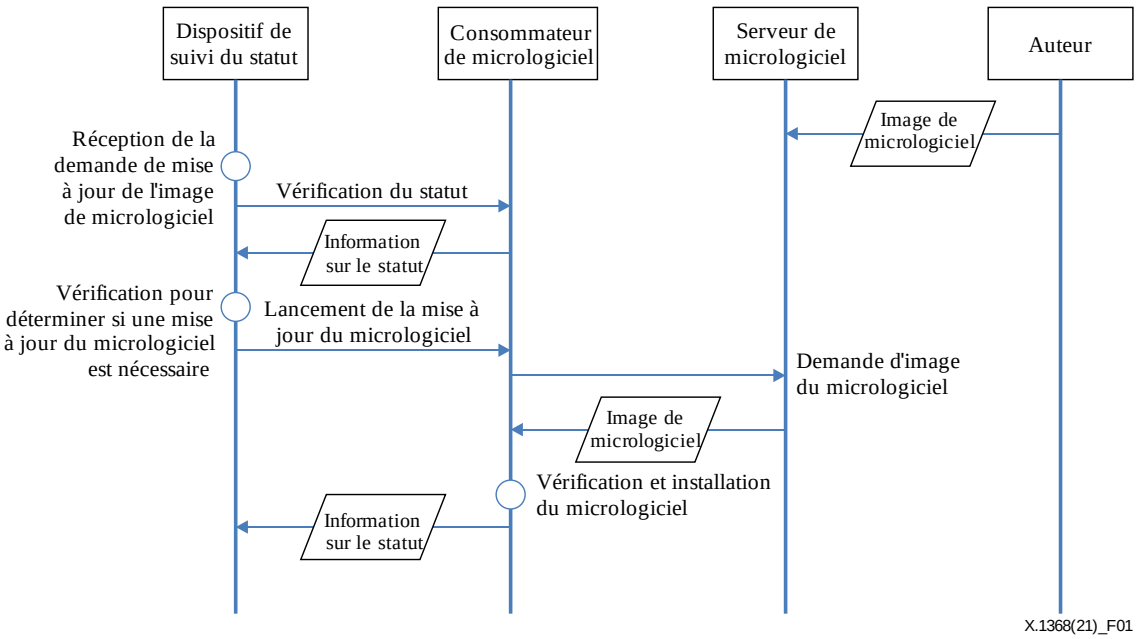

Figure 1 – Procédure du protocole

8 Scénarios de déploiement

Comme indiqué au § 6, plusieurs entités fonctionnelles peuvent se trouver à l'intérieur d'un même nœud, et plusieurs entités peuvent faire fonction d'entité fonctionnelle; les scénarios de déploiement peuvent différer selon les cas. Dans le présent paragraphe, plusieurs scénarios de déploiement sont illustrés.

8.1 Entités fonctionnelles à l'intérieur des dispositifs IoT

La Figure 2 illustre quatre types de dispositifs IoT. Un dispositif IoT doit contenir au moins un consommateur de micrologiciel, car il est normal qu'un dispositif IoT contienne plusieurs images de micrologiciel.

Un dispositif IoT doit contenir au moins un dispositif de suivi du statut. Il pourrait contenir plusieurs dispositifs de suivi du statut pour traiter plusieurs consommateurs de micrologiciel, mais un seul dispositif de suivi du statut qui traite tous les consommateurs de micrologiciel fonctionne également de manière satisfaisante.

Un dispositif IoT à ressources limitées peut souhaiter limiter au minimum la fonctionnalité du dispositif de suivi du statut. En pareil cas, la fonctionnalité du dispositif de suivi du statut est subdivisée en un module côté client et un module côté serveur déployés en dehors du dispositif IoT. Les fonctionnalités minimales, par exemple les interactions avec un consommateur de micrologiciel, demeurent côté client, tandis que les autres fonctionnalités sont exportées côté serveur. Un module côté serveur peut prendre en charge plusieurs modules côté client. Il s'agit souvent du type de déploiement préféré.

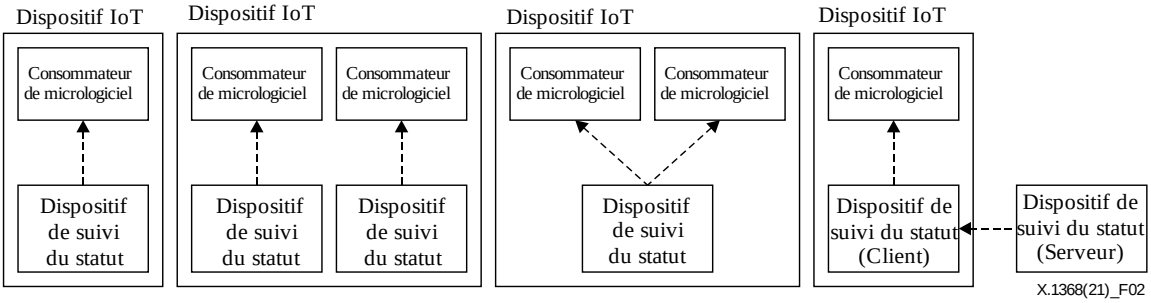

Figure 2 – Différents types de dispositif IoT

8.2 Types de déploiement de dispositif de suivi du statut

Les ressources des dispositifs IoT diffèrent considérablement; un dispositif de suivi du statut peut se trouver à l'intérieur d'un dispositif IoT, mais les dispositifs IoT à ressources limitées peuvent souhaiter maintenir un dispositif de suivi à part et réduire au minimum sa consommation de ressources. En outre, dans certains cas, il pourrait être préférable que les dispositifs IoT soient gérés par une entité centralisée pour plus de commodité.

Pour faire face à ces situations, un dispositif de suivi du statut peut être subdivisé en plusieurs modules et mis en œuvre de manière hiérarchique. En pareil cas, plusieurs modules peuvent être mis en cascade, afin qu'un module en amont puisse déterminer si une mise à jour du micrologiciel est nécessaire et lancer la procédure correspondante par l'intermédiaire des modules en aval.

Les cas dans lesquels: 1) un dispositif de suivi du statut à l'intérieur d'un dispositif IoT communique directement avec un serveur de micrologiciel, 2) un dispositif de suivi du statut à l'intérieur d'un dispositif IoT communique avec un serveur de micrologiciel via un autre dispositif de suivi du statut se trouvant dans l'Intranet, et 3) un dispositif de suivi du statut à l'intérieur d'un dispositif IoT communique avec un serveur de micrologiciel via plusieurs dispositifs de suivi du statut sont examinés aux § 8.2.1 à 8.2.3.

8.2.1 Modèle de suivi du statut intra-dispositif

La Figure 3 illustre le modèle de suivi du statut intra-dispositif. Dans ce modèle, un consommateur de micrologiciel et un dispositif de suivi du statut se trouvent à l'intérieur d'un dispositif IoT. Lorsque le dispositif de suivi du statut comprend qu'il faut mettre à jour le micrologiciel (voir le § 9), il demande au consommateur de micrologiciel de recevoir des images de micrologiciel en provenance du serveur de micrologiciel. Il convient de noter que les canaux de communication sont résumés dans

cette section, mais qu'ils pourraient être connectés via le protocole Internet ou d'autres protocoles, ou une combinaison de ceux-ci qui nécessite des ponts pour les communications entre les entités. La Figure 3 porte sur l'Internet, mais les techniques indiquées dans la présente Recommandation peuvent également prendre en charge toutes sortes d'autres réseaux.

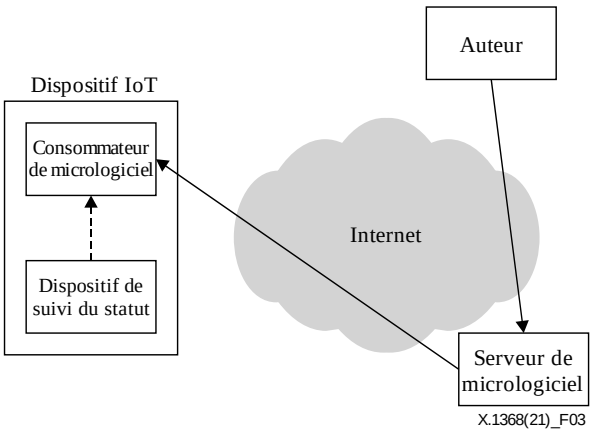

Figure 3 – Déploiement à titre d'exemple d'un modèle de suivi du statut intra-dispositif

8.2.2 Modèle de suivi du statut client-serveur

La Figure 4 illustre le modèle de suivi du statut client-serveur. Dans ce modèle, un système de suivi du statut est subdivisé en un module client et un module serveur. Les modules clients se trouvent dans les dispositifs IoT, tandis qu'un module serveur se trouve à l'intérieur d'un réseau. Le module serveur surveille plusieurs dispositifs IoT en communiquant avec les modules clients. Les modules clients se contentent de vérifier le message provenant du module serveur et agissent en conséquence. Le module serveur lance la procédure de mise à jour du micrologiciel.

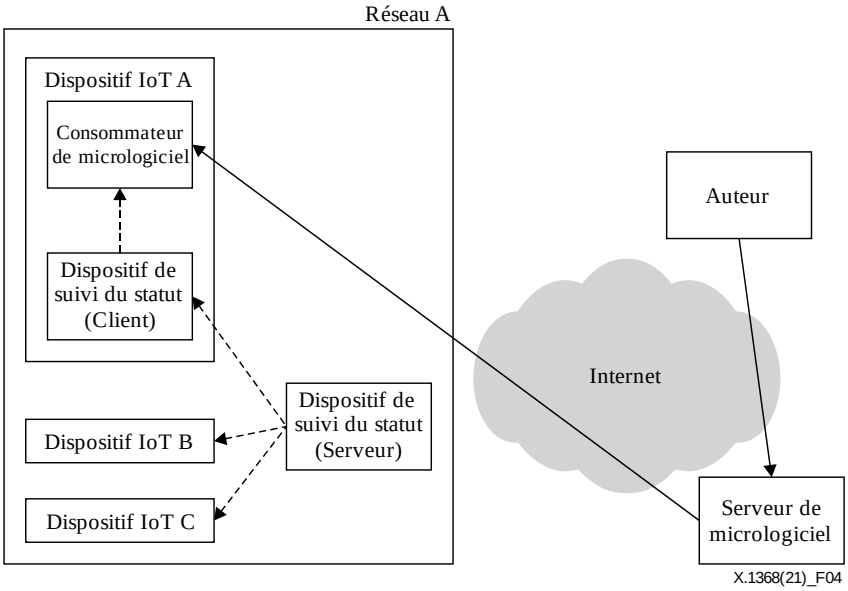

Figure 4 – Déploiement à titre d'exemple d'un modèle de suivi du statut client-serveur

8.2.3 Modèle de suivi du statut hiérarchique

La Figure 5 illustre le modèle de suivi du statut hiérarchique. Dans ce modèle, un système de suivi du statut est subdivisé en plusieurs modules: module client, modules intermédiaires et module serveur. Les modules clients se trouvent dans les dispositifs IoT, tandis que le module serveur et les modules intermédiaires se trouvent à l'intérieur des réseaux. Les modules intermédiaires surveillent plusieurs dispositifs IoT et le module serveur, en communiquant avec les modules clients, surveille

tous les modules clients en communiquant avec les modules intermédiaires. À noter que les modules intermédiaires peuvent être mis en cascade pour générer une hiérarchie supplémentaire. Les modules clients se contentent de vérifier le message du module serveur et agissent en conséquence. Le module serveur lance la procédure de mise à jour du micrologiciel. Le module serveur lance la procédure de mise à jour du micrologiciel.

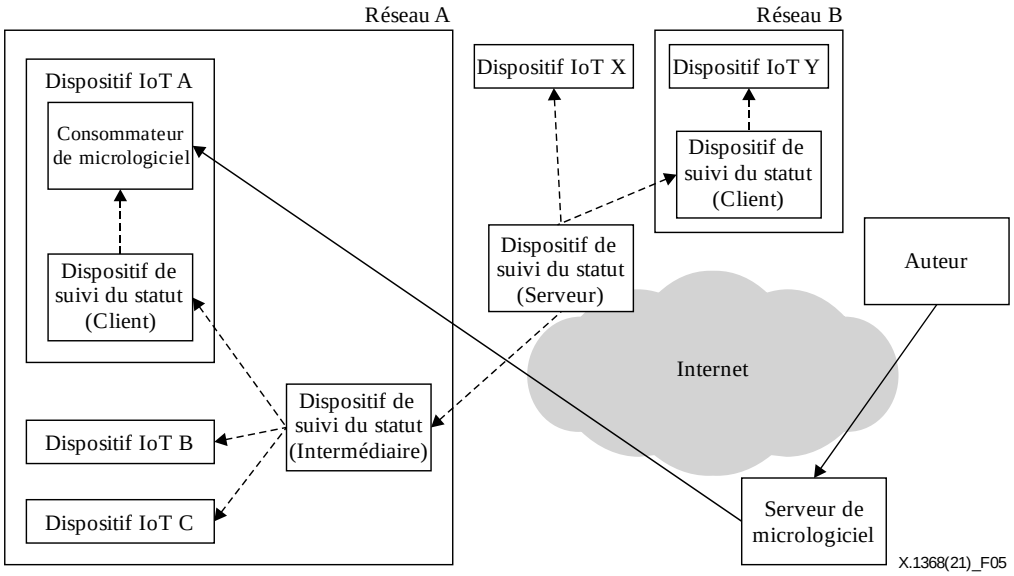

Figure 5 – Déploiement à titre d'exemple d'un modèle de suivi du statut hiérarchique

9 Découverte de nouvelles images de micrologiciel disponibles et déclenchement de la procédure

L'ensemble du processus est lancé par un dispositif de suivi du statut lorsqu'il reçoit une demande de mise à jour de l'image de micrologiciel. Ce type de demande peut revêtir différentes formes:

a) Un auteur qui publie de nouvelles versions d'images de micrologiciel peut envoyer la demande.

b) Un serveur de micrologiciel qui reçoit une nouvelle version d'une image de micrologiciel peut envoyer la demande.

c) Un administrateur de dispositif IoT reconnaît la publication d'une nouvelle version des images de micrologiciel et peut envoyer la demande.

d) Un dispositif de suivi du statut ou l'un de ses dispositifs de suivi du statut en amont découvre la nouvelle version des images de micrologiciel en interrogeant périodiquement le serveur de micrologiciel.

e) Un dispositif de suivi du statut ou l'un de ses dispositifs de suivi du statut en amont reconnaît l'existence d'une nouvelle version de l'image de micrologiciel en observant une procédure de mise à jour du micrologiciel d'un autre dispositif IoT dont il s'occupe.

Plusieurs autres événements peuvent émettre les demandes, mais celles-ci doivent fournir des informations sur l'adresse URL des images de micrologiciel et leurs versions au dispositif de suivi du statut. Si le dispositif de suivi du statut établit que les informations sont fiables et dignes de confiance, il peut engager la procédure visée au § 7.

10 Exigences

Dans le présent paragraphe, on énumère les exigences fonctionnelles applicables aux mises à jour des logiciels de l'IoT. En raison de contraintes liées aux ressources, les procédures de mise à jour des logiciels disponibles dans un environnement qui n'est pas soumis à des contraintes ne sont pas toutes

applicables. Il arrive souvent qu'aucun utilisateur ou opérateur humain ne se trouve à proximité des dispositifs IoT. Par conséquent, lors de la conception de la procédure concrète de mise à jour de sécurité, il faut prendre en compte ces différences. Il convient de noter que la confidentialité, l'intégrité et la disponibilité des quatre entités fonctionnelles doivent être préservées, et constituent des conditions préalables à la mise à jour des logiciels; elles sont donc omises des exigences énumérées ci-après.

a) Les logiciels/micrologiciels malveillants ne doivent pas être distribués:
   i) les images malveillantes devraient être identifiées avant d'être téléchargées ou échangées;
   ii) l'intégrité des images de micrologiciel doit pouvoir être vérifiée;
   iii) le fournisseur d'images de micrologiciel doit pouvoir être vérifié.

b) Les logiciels/micrologiciels vulnérables doivent faire l'objet de mesures appropriées:
   i) les versions obsolètes des logiciels/micrologiciels devraient être détectées;
   ii) les logiciels/micrologiciels vulnérables devraient être détectés.

c) Il doit être possible d'effectuer une reprise dans le cas d'une défaillance pendant la procédure de mise à jour:
   i) en cas d'échec d'une mise à jour de logiciel/micrologiciel, il devrait y avoir un moyen de notifier cette situation;
   ii) il devrait y avoir un moyen de repli ou de protection en cas d'échec du processus de mise à jour.

d) Seule la mise à jour prévue et nécessaire devrait être effectuée:
   i) seules les versions les plus récentes des logiciels/micrologiciels de l'IoT doivent pouvoir être installées;
   ii) seules les images fiables des logiciels/micrologiciels de l'IoT doivent pouvoir être installées.

e) Les contraintes en matière de ressources doivent être prises en considération:
   i) une procédure de mise à jour ne devrait pas avoir lieu si elle n'est pas nécessaire, de façon à réduire au minimum les ressources du réseau;
   ii) les fonctions du dispositif de suivi du statut peuvent être mises en cascade, pour réduire au minimum les contraintes liées aux dispositifs IoT à ressources limitées.

f) Les droits de propriété intellectuelle des auteurs doivent être préservés:
   i) les images de logiciels/micrologiciels doivent être chiffrées par les auteurs;
   ii) la confidentialité, l'intégrité et la disponibilité des images de logiciels/micrologiciels de l'IoT doivent être préservées.
   iii) les images de logiciels/micrologiciels doivent être transférées en toute sécurité de l'auteur à la destination finale.

11 Capacités

Sur la base des exigences indiquées au § 10, on énumère dans le présent paragraphe les capacités des entités fonctionnelles.

11.1 Capacités d'un consommateur de micrologiciel

a) Un consommateur de micrologiciel devrait pouvoir:
   i) vérifier si l'exécution précédente d'une mise à jour de micrologiciel a été effectuée avec succès;

ii) partager les informations sur ses images de logiciel/micrologiciel actuelles (par exemple, le numéro de version) avec les parties qui demandent ces informations avec des droits légitimes;

iii) mettre en place un moyen de repli ou de protection en cas d'échec du processus de mise à jour;

iv) informer le dispositif de suivi du statut de la nécessité d'une mise à jour du micrologiciel;

v) confirmer l'authenticité et l'intégrité des images de micrologiciel en vérifiant lui-même leurs certificats ou par d'autres moyens (par exemple, en déléguant le processus de vérification à d'autres entités);

vi) choisir de ne pas installer la nouvelle version des images de logiciel/micrologiciel.

b) Il est recommandé à un consommateur de micrologiciel de disposer d'un "mode sécurisé" qui fait fonctionner le dispositif IoT avec un minimum de fonctionnalités et qui offre au moins un moyen d'installer, de rétablir ou de mettre à jour manuellement le micrologiciel.

11.2 Capacités d'un dispositif de suivi du statut

Un dispositif de suivi du statut devrait pouvoir:

a) tenir à jour des listes de consommateurs de micrologiciels, à savoir ceux dont les images de micrologiciels sont à jour et ceux dont les images de micrologiciels sont obsolètes:

i) ces listes devraient contenir au minimum leurs identifiants uniques;

ii) un dispositif de suivi du statut devrait être en mesure d'identifier les consommateurs de micrologiciel dont le micrologiciel est obsolète;

b) connaître le statut des consommateurs de micrologiciel qu'il gère. Il devrait exister un moyen:

i) de confirmer si le consommateur de micrologiciel (et le dispositif IoT qui contient le consommateur de micrologiciel) est prêt, en communiquant avec le consommateur de micrologiciel et en vérifiant les journaux de communication avec le consommateur de micrologiciel;

ii) de confirmer si l'exécution précédente d'une mise à jour de micrologiciel au niveau d'un consommateur de micrologiciel a été effectuée avec succès;

iii) de connaître les versions du micrologiciel que les consommateurs de micrologiciel utilisent;

c) déterminer si une mise à jour de logiciel/micrologiciel est nécessaire et lancer une procédure de mise à jour de micrologiciel lorsque cela est nécessaire;

d) vérifier l'authenticité d'un dispositif de suivi du statut en amont lorsqu'il est mis en œuvre de manière hiérarchique.

Lorsque la fonctionnalité d'un dispositif de suivi du statut est subdivisée en plusieurs modules, ces modules doivent pouvoir:

a) maintenir la confidentialité et l'intégrité de la communication entre eux;

b) vérifier l'authenticité des signaux qu'ils s'envoient mutuellement;

c) tenir à jour leurs informations d'accessibilité.

11.3 Capacités d'un serveur de micrologiciel

Un serveur de micrologiciel devrait pouvoir:

a) accepter les soumissions d'images de logiciels/micrologiciels de l'IoT des auteurs;

b) fournir les images de logiciels/micrologiciels qu'il contient aux consommateurs de micrologiciels;

c) identifier les images de logiciels/micrologiciels malveillants et prendre les mesures appropriées, par exemple en les retirant de son stockage interne et en interdisant la soumission par les auteurs qui soumettent ces images;

d) gérer la liste des auteurs et des consommateurs de micrologiciels qui l'utilisent;

e) gérer les versions des images de logiciels/micrologiciels de l'IoT;

f) tenir à jour la liste des consommateurs de micrologiciel et des images de logiciels/micrologiciels qu'ils ont téléchargées dans le passé;

g) informer les dispositifs IoT qui ont téléchargé dans le passé des logiciels/micrologiciels de l'IoT obsolètes que de nouvelles versions sont disponibles;

h) vérifier l'emplacement géographique ou logique des dispositifs IoT et autoriser ou refuser le téléchargement d'images de logiciels/micrologiciels, afin d'éviter de les distribuer dans des emplacements interdits identifiés par des politiques ou d'autres moyens.

11.4 Capacités d'un auteur

Un auteur devrait pouvoir maintenir l'authenticité, la confidentialité et l'intégrité des images de micrologiciel qu'il a produites.

a) Un micrologiciel ne devrait pas être remplacé ou compromis par des tiers (authenticité et intégrité).

b) La propriété intellectuelle des fournisseurs dans le micrologiciel devrait être préservée (confidentialité).

c) Un auteur devrait mettre en œuvre des mesures pour sécuriser l'image de micrologiciel qu'il télécharge sur les serveurs de micrologiciel, étant donné qu'un serveur de micrologiciel n'est pas nécessairement fiable.

Appendice I

Activités connexes hors du cadre de l'UIT-T

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

Les activités relatives aux mises à jour des logiciels de l'IoT qui ont été étudiées hors du cadre de l'UIT-T sont les suivantes:

1) Atelier sur l'IOTSU [b-ISOC ioTSU];

2) Groupe de travail SUIT de l'IETF [b-IETF suit]:
   - sur le fichier "manifeste" [b-IETF manifest];
   - sur la mise à jour de l'architecture de micrologiciel [b-IETF architecture];

3) oneM2M: Normes relatives aux communications de machine à machine (M2M) et l'IoT [b-oneM2M] etc.

Appendice II

Exemple de scénario de mise à jour de logiciel de l'IoT au moyen de la technologie des registres distribués

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

II.1 Aperçu

L'infrastructure IoT contient un grand nombre de dispositifs qu'un administrateur doit gérer. Un dispositif IoT fait l'objet de diverses révisions, selon les caractéristiques du matériel, et différents micrologiciels peuvent être appliqués, selon la carte de capteur additionnelle. De plus, la version logicielle prise en charge diffère en fonction de la version du matériel. Les différences dans les progiciels installés peuvent également poser des problèmes de dépendance, qui peuvent être résolus moyennant l'utilisation de la technologie des registres distribués (DLT).

Grâce à la technologie DLT, il existe un contrat intelligent qui permet d'effectuer des mises à jour micrologicielles ou logicielles du matériel sur la base de contrats pré-rédigés par l'administrateur. En outre, il peut être remédié aux failles de sécurité qui peuvent se produire pendant le processus de mise à jour sur la base d'algorithmes de consensus et de la couche cryptographique.

Cet exemple décrit la façon de fournir des mises à jour de micrologiciel/logiciel sécurisées sur la base de la technologie DLT, dans des environnements qui se caractérisent par des révisions du matériel et des versions logicielles différentes, comme l'infrastructure IoT.

II.2 Procédure de mise à jour du logiciel

Voir le Tableau II.1 et les Figures II.1 et II.2.

Tableau II.1 – Structure de bloc pour la mise à jour du logiciel

En-tête de bloc	− Longueur de bloc, version − Hachage précédent de l'en-tête de bloc
Données de bloc	− Racine de Merkle − Nom du fournisseur, heure de publication, numéro de version, code de hachage du fichier, lien du fichier, nom du fichier, taille du fichier, matériel d'appui, dépendance du logiciel

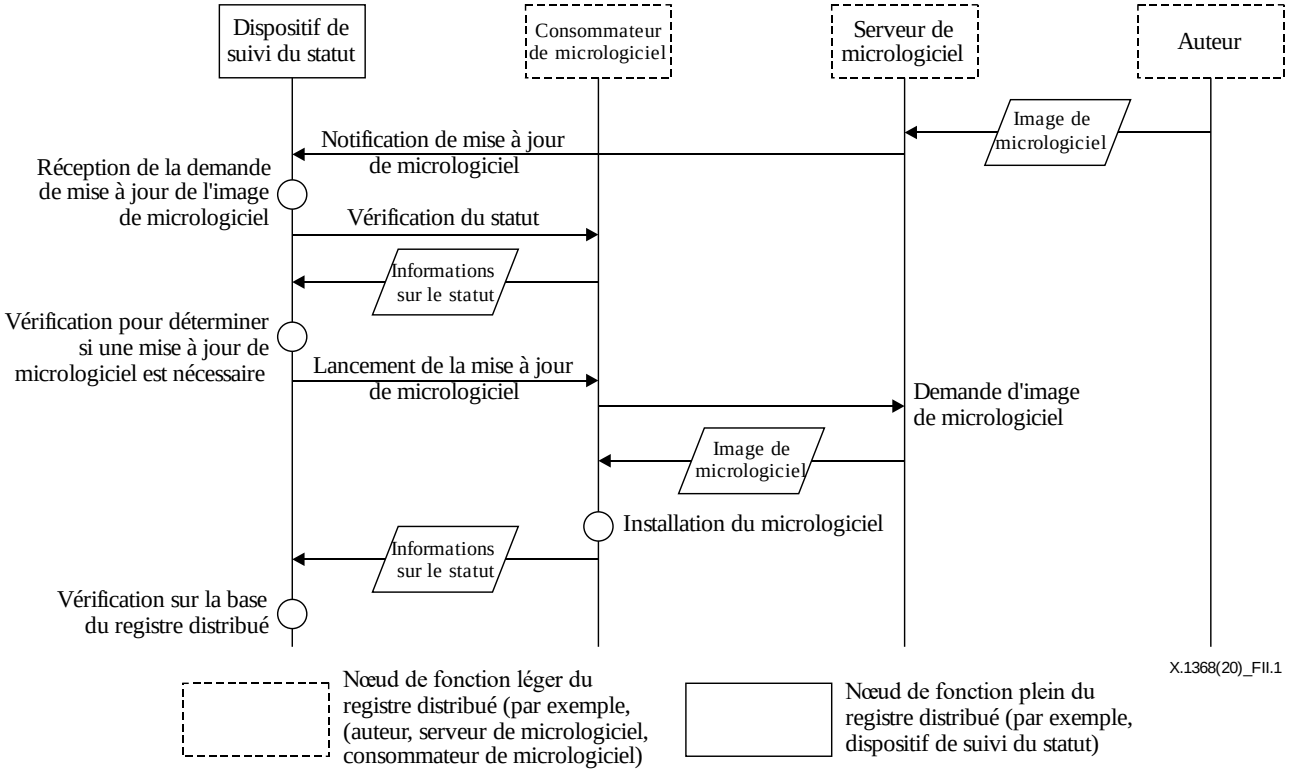

Figure II.1 – Procédure de mise à jour de logiciel sur la base des registres distribués

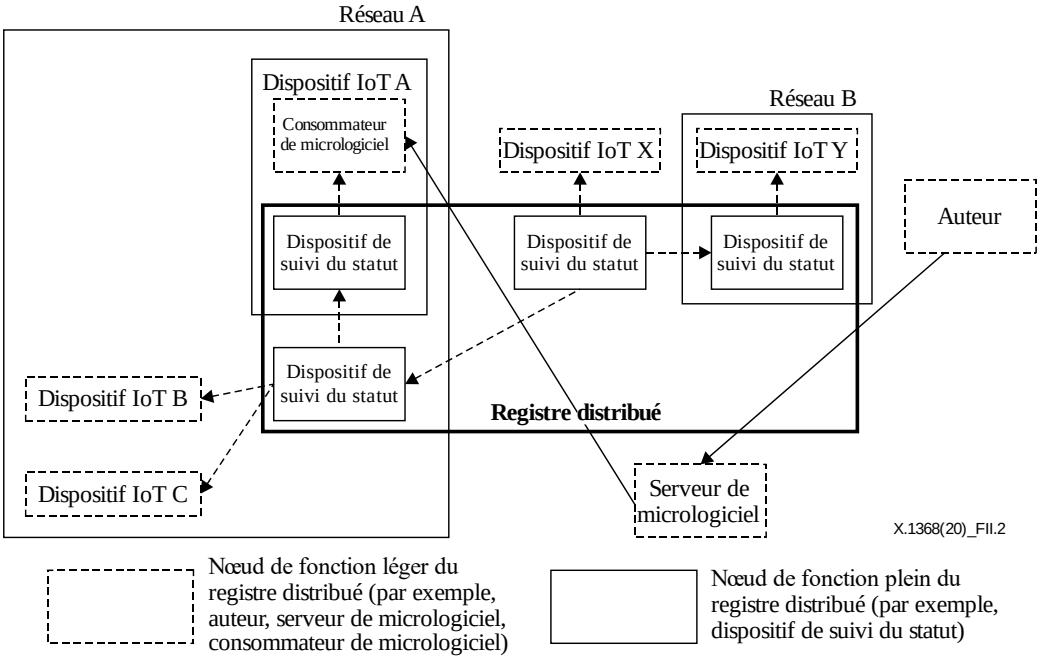

Figure II.2 – Mise à jour de logiciel sur la base des registres distribués pour plusieurs réseaux

Bibliographie

[b-IETF RFC 2119] IETF RFC 2119 (1997), *Key words for use in RFCs to indicate requirement levels.*

[b-IETF architecture] IETF SUIT (2019). *A firmware update architecture for Internet of things*, Wilmington, DE: Internet Engineering Task Force. Disponible à l'adresse [consultée le 19/02/2021]: https://tools.ietf.org/html/draft-ietf-suit-architecture-08

[b-IETF manifest] Moran, B., Tschofenig, H., Birkholz, H. (2019). *Firmware updates for Internet of things devices – An information model for manifests.* Wilmington, DE: Internet Engineering Task Force. Disponible à l'adresse [consultée le 19/02/2021]: https://tools.ietf.org/id/draft-ietf-suit-information-model-02.html

[b-IETF suit] IETF (2021). *Software updates for the internet of things (suit)*, version 7.26.0. Wilmington, DE: Internet Engineering Task Force. Disponible à l'adresse [consultée le 19/02/2021]: https://datatracker.ietf.org/wg/suit/about/

[b-ISOC iotsu] Internet Architecture Board (Internet), *Internet of things software update workshop (IoTSU) 2016*. Reston, VA: Internet Society. Disponible à l'adresse [consultée le 20/02/2021]: https://www.iab.org/activities/workshops/iotsu/

[b-oneM2M] oneM2M (2017), *Standards for M2M and the Internet of things*. oneM2M. Disponible à l'adresse [consultée le 20/02/2021]: http://www.onem2m.org/technical/published-drafts

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	Équipements 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, 2021