Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.4908

(12/2020)

SÉRIE Y: INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

Internet des objets et villes et communautés intelligentes – Évaluation et analyse

Cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté dans l'Internet des objets

Recommandation UIT-T Y.4908

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET, RÉSEAUX DE PROCHAINE GÉNÉRATION, INTERNET DES OBJETS ET VILLES INTELLIGENTES

INFRASTRUCTURE MONDIALE DE L'INFORMATION	
Généralités	Y.100–Y.199
Services, applications et intergiciels	Y.200–Y.299
Aspects réseau	Y.300–Y.399
Interfaces et protocoles	Y.400–Y.499
Numérotage, adressage et dénomination	Y.500–Y.599
Gestion, exploitation et maintenance	Y.600–Y.699
Sécurité	Y.700–Y.799
Performances	Y.800–Y.899
ASPECTS RELATIFS AU PROTOCOLE INTERNET	
Généralités	Y.1000–Y.1099
Services et applications	Y.1100–Y.1199
Architecture, accès, capacités de réseau et gestion des ressources	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interfonctionnement	Y.1400–Y.1499
Qualité de service et performances de réseau	Y.1500–Y.1599
Signalisation	Y.1600–Y.1699
Gestion, exploitation et maintenance	Y.1700–Y.1799
Taxation	Y.1800–Y.1899
Télévision IP sur réseaux de prochaine génération	Y.1900–Y.1999
RÉSEAUX DE PROCHAINE GÉNÉRATION	
Cadre général et modèles architecturaux fonctionnels	Y.2000–Y.2099
Qualité de service et performances	Y.2100–Y.2199
Aspects relatifs aux services: capacités et architecture des services	Y.2200–Y.2249
Aspects relatifs aux services: interopérabilité des services et réseaux dans les réseaux de prochaine génération	Y.2250–Y.2299
Améliorations concernant les réseaux de prochaine génération	Y.2300–Y.2399
Gestion de réseau	Y.2400–Y.2499
Architectures et protocoles de commande de réseau	Y.2500–Y.2599
Réseaux de transmission par paquets	Y.2600–Y.2699
Sécurité	Y.2700–Y.2799
Mobilité généralisée	Y.2800–Y.2899
Environnement ouvert de qualité opérateur	Y.2900–Y.2999
RÉSEAUX FUTURS	Y.3000–Y.3499
INFORMATIQUE EN NUAGE	Y.3500–Y.3999
MÉGADONNÉES	Y.3600–Y.3799
RÉSEAUX DE DISTRIBUTION DE CLÉS QUANTIQUES	Y.3800–Y.3999
INTERNET DES OBJETS ET VILLES ET COMMUNAUTÉS INTELLIGENTES	
Considérations générales	Y.4000–Y.4049
Termes et définitions	Y.4050–Y.4099
Exigences et cas d'utilisation	Y.4100–Y.4249
Infrastructure, connectivité et réseaux	Y.4250–Y.4399
Cadres, architectures et protocoles	Y.4400–Y.4549
Services, applications, calcul et traitement des données	Y.4550–Y.4699
Gestion, commande et qualité de fonctionnement	Y.4700–Y.4799
Identification et sécurité	Y.4800–Y.4899
Évaluation et analyse	**Y.4900-Y.4999**

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

Recommandation UIT-T Y.4908

Cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté dans l'Internet des objets

Résumé

Les gouvernements et les parties prenantes mettent actuellement en place des systèmes de cybersanté afin d'accroître l'efficacité, l'efficience et la qualité des services de soins de santé. L'Internet des objets, technologie relativement nouvelle, permet de faire évoluer les systèmes de cybersanté afin d'améliorer encore les services de soins de santé. Toutefois, pour cette évolution, il est nécessaire de disposer de cadres permettant d'évaluer efficacement la qualité de fonctionnement des systèmes de cybersanté faisant partie de l'Internet des objets.

La Recommandation UIT-T Y.4908 répond à ce besoin et inclut:

– une classification des services de cybersanté faisant partie de l'Internet des objets;

– un ensemble non exhaustif de critères non fonctionnels d'évaluation de la qualité de fonctionnement applicables aux systèmes de cybersanté appartenant à l'Internet des objets;

– des cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté appartenant à l'Internet des objets.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	UIT-T Y.4908	16-12-2020	20	11.1002/1000/14425

Mots clés

Classification des services de cybersanté faisant partie de l'Internet des objets; critères d'évaluation de la qualité de fonctionnement; cadre d'évaluation de la qualité de fonctionnement.

* 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

Recommandation UIT-T Y.4908

Cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté dans l'Internet des objets

1 Domaine d'application

Le domaine d'application de la présente Recommandation comprend les éléments suivants:

– une classification des services de cybersanté faisant partie de l'Internet des objets (IoT);

– un ensemble non exhaustif de critères non fonctionnels d'évaluation de la qualité de fonctionnement (interopérabilité, facilité d'utilisation, sécurité) applicables aux systèmes de cybersanté appartenant à l'Internet des objets;

– un cadre d'évaluation de la qualité de fonctionnement des systèmes de cybersanté appartenant à l'Internet des objets.

Les exigences et capacités techniques précises des systèmes de cybersanté faisant partie de services de soins de santé généraux n'entrent pas dans le domaine d'application de la présente Recommandation.

Les exigences d'ordre réglementaire ne font pas partie du domaine d'application de la présente Recommandation.

La présente Recommandation n'impose aucune méthode d'évaluation en particulier. Elle laisse volontairement au praticien une marge de manœuvre suffisante pour utiliser un ou plusieurs critères d'évaluation de la qualité de fonctionnement définis ci-après.

Les cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté généraux n'entrent pas non plus dans le domaine d'application de la présente Recommandation.

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 se reporter, si possible, aux versions les plus récentes des Recommandations et autres références énumérées ci-dessous. La liste des Recommandations de l'UIT-T en vigueur est régulièrement publiée. La référence à un document figurant dans la présente Recommandation ne donne pas à ce document, en tant que tel, le statut d'une Recommandation.

[UIT-T Y.4000] Recommandation UIT-T Y.4000/Y.2060 (2012), *Présentation générale de l'Internet des objets.*

[UIT-T Y.4110] Recommandation UIT-T Y.4110/Y.2065 (2014), *Exigences relatives aux services et aux capacités pour les services de suivi utilisant la cybersanté.*

[UIT-T Y.4113] Recommandation UIT-T Y.4113 (2016), *Exigences applicables au réseau pour l'Internet des objets.*

[UIT-T Y.4408] Recommandation UIT-T Y.4408/Y.2075 (2015), *Cadre des capacités pour les services de suivi dans le domaine de la cybersanté.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation emploie les termes suivants définis ailleurs:

3.1.1 dispositif [UIT-T Y.4000]: dans l'Internet des objets, équipement doté obligatoirement de capacités de communication et éventuellement de capacités de détection, d'actionnement, de saisie de données, de stockage de données et de traitement de données.

3.1.2 Internet des objets (IoT) [UIT-T Y.4000]: infrastructure mondiale pour la société de l'information, qui permet de disposer de services évolués en interconnectant des objets (physiques ou virtuels) grâce aux technologies de l'information et de la communication interopérables existantes ou en évolution.

NOTE 1 – En exploitant les capacités d'identification, de saisie de données, de traitement et de communication, l'IoT tire pleinement parti des objets pour offrir des services à toutes sortes d'applications, tout en garantissant le respect des exigences de sécurité.

NOTE 2 – Dans une optique plus large, l'IoT peut être considéré comme un concept ayant des répercussions sur les technologies et la société.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis dans la présente Recommandation:

3.2.1 prestataire de services de cybersanté: organisation qui fournit des services de cybersanté conçus pour les organisations aux organisations clientes de services de cybersanté et/ou des services de cybersanté conçus pour les particuliers aux particuliers clients de services de cybersanté.

3.2.2 organisation cliente de services de cybersanté: organisation cliente de services de cybersanté conçus pour les organisations et fournis par un prestataire de services de cybersanté.

3.2.3 particulier client de services de cybersanté: personne cliente de services de cybersanté conçus pour les particuliers et fournis par un prestataire de services de cybersanté.

3.2.4 fournisseur de solutions de cybersanté: organisation qui produit les logiciels et le matériel nécessaires aux prestataires de services de cybersanté et aux organisations clientes de services de cybersanté et/ou aux particuliers clients de services de cybersanté, afin de mettre en place des services de cybersanté.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

API interface de programmation d'application (*application programming interface*)

IoT Internet des objets (*Internet of Things*)

JSON notation des objets en JavaScript (*JavaScript object notation*)

QoS qualité de service (*quality of service*)

SLA accord de niveau de service (*service level agreement*)

SSAS prise en charge des services et des applications (*service support and application support*)

TIC technologies de l'information et de la communication

XML langage de balisage extensible (*extensible markup language*)

5 Conventions

Aucune.

6 Services et systèmes de cybersanté appartenant à l'Internet des objets

6.1 Présentation des services et systèmes de cybersanté dans l'Internet des objets

Les services de cybersanté s'inscrivent dans le prolongement des services de santé classiques (par exemple les services de suivi utilisant la cybersanté [UIT-T Y.4110], la gestion sanitaire en ligne et les consultations à distance).

Dans la présente Recommandation, les systèmes de cybersanté désignent un mélange d'applications, de dispositifs et de serveurs, qui fonctionnent grâce à des technologies de l'information et de la communication connexes (comme les réseaux, les données et les interfaces de programmation d'application (API)) utilisées pour fournir des services de cybersanté.

Il existe différents types de systèmes de cybersanté. Certains sont utilisés dans une optique d'administration de la santé, comme les systèmes destinés aux établissements d'administration sanitaire, tandis que d'autres sont utilisés pour dispenser des soins, comme les systèmes destinés aux hôpitaux et aux établissements de soins de santé. Dans la présente Recommandation, les dispositifs de santé individuels tels que les téléphones intelligents équipés de capteurs sont considérés comme des systèmes de cybersanté particuliers qui aident les personnes à mieux gérer leur état de santé.

L'Internet des objets (IoT) [UI-T Y.4000] fournit une infrastructure mondiale pour la société de l'information dont l'objectif est d'améliorer les interactions des systèmes de cybersanté.

À la différence des systèmes de cybersanté qui n'ont pas les capacités conférées par l'IoT, les systèmes de cybersanté faisant partie de l'IoT (c'est-à-dire les systèmes de cybersanté qui ont des capacités conférées par l'IoT) peuvent s'interconnecter efficacement. L'infrastructure de l'IoT comprend en particulier des mécanismes d'interopérabilité communs qui font gagner du temps et évitent d'avoir à trop modifier le code.

Le schéma de gauche a) de la Figure 1 donne un exemple typique d'un service de cybersanté général (c'est-à-dire un service de cybersanté ne faisant pas partie de l'IoT), dans lequel les systèmes de cybersanté associés disposent d'une connexion directe (entre homologues) avec les différentes parties prenantes de la cybersanté (en général un établissement de santé, un hôpital et les particuliers). Dans ce cas, les interfaces (par exemple les interfaces API), les formats de données, les interactions entre les entités et d'autres aspects connexes doivent être définis et mis au point au cas par cas.

Le schéma de droite b) de la Figure 1 illustre le cas d'un service de cybersanté faisant partie de l'IoT, dans lequel différents systèmes de cybersanté (mis en place par différentes parties prenantes) sont interconnectés au moyen d'une plate-forme IoT de cybersanté centralisée (qui peut être considérée comme faisant partie de l'infrastructure IoT), aussi appelée plate-forme de prise en charge des services et des applications (SSAS). Dans ce cas, la plate-forme SSAS gère les problèmes d'hétérogénéité (par exemple en ce qui concerne les interfaces, les formats de données et fonctionnalités d'interaction) entre les divers systèmes de cybersanté associés.

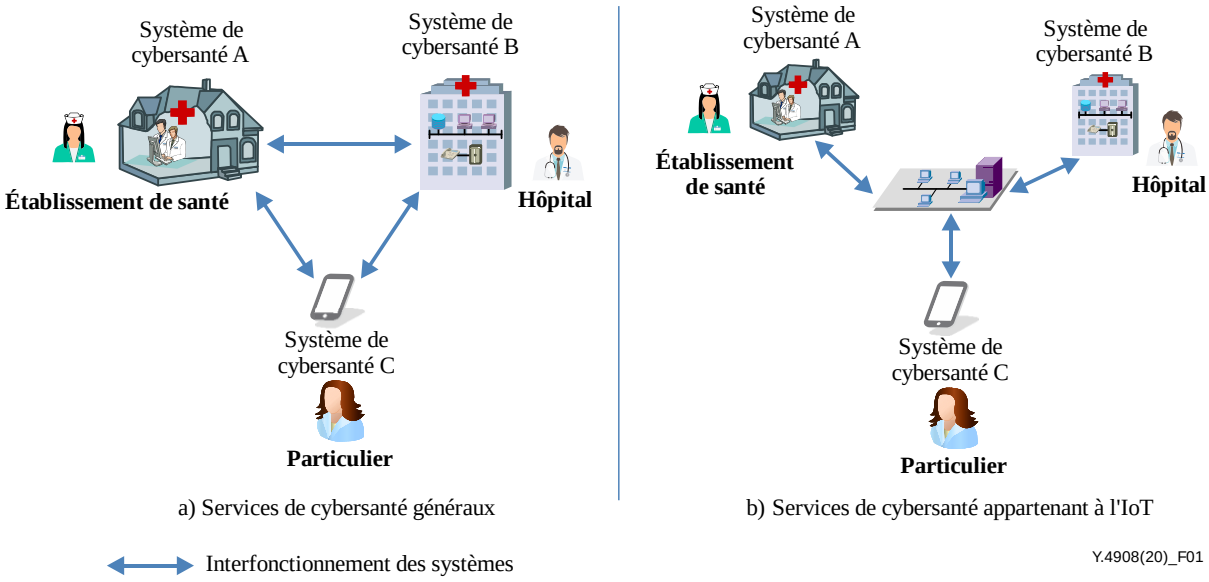

Figure 1 – Exemples de services de cybersanté généraux et de services de cybersanté dans l'IoT

6.2 Classification des services de cybersanté dans l'IoT

Compte tenu des différents profils d'utilisateurs et des équipements techniques, on peut distinguer trois types de services de cybersanté appartenant à l'IoT, à savoir:

– les services de cybersanté centrés sur les personnes;

– les services de cybersanté centrés sur les organisations; et

– les services de cybersanté centrés sur la population.

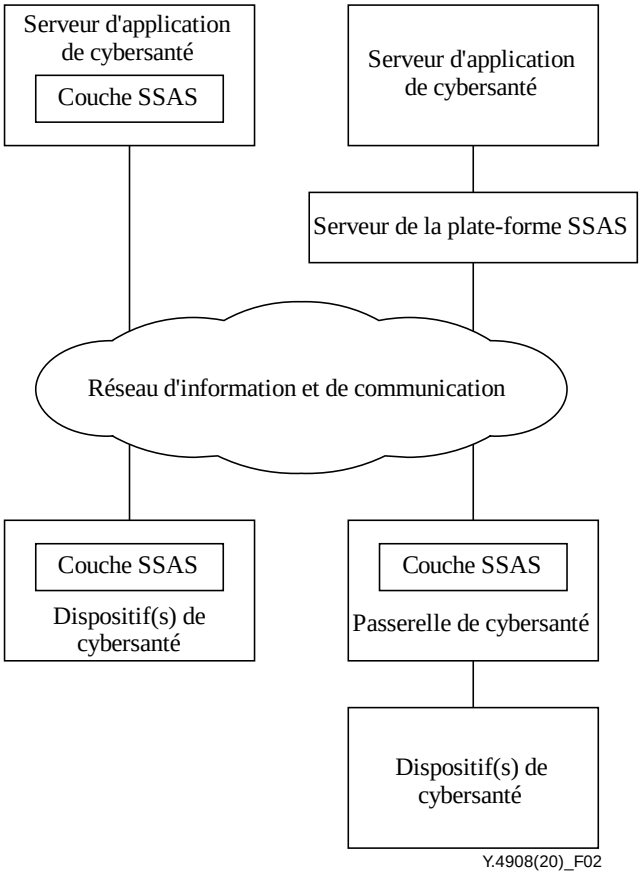

Figure 2 – Architecture d'un système de services de cybersanté appartenant à l'IoT [UIT-T Y.4113] et des composants associés

Services de cybersanté centrés sur les personnes: l'accent est mis sur les personnes, qui sont les principaux utilisateurs de ce type de services de cybersanté. En tant qu'utilisateurs des services de cybersanté centrés sur les personnes, celles-ci se concentrent essentiellement sur les fonctionnalités, la compatibilité, la consommation d'énergie, la sécurité, la confidentialité et le coût du ou des dispositif(s) de cybersanté ainsi que sur l'état du réseau d'information et de communication (par exemple la couverture, l'assurance d'une bonne qualité de service et le coût). Le ou les dispositif(s) de cybersanté, la passerelle de cybersanté et le réseau d'information et de communication sont les principaux composants des services de cybersanté centrés sur les personnes.

Services de cybersanté centrés sur les organisations: l'accent est mis sur les organisations, qui sont les principaux utilisateurs de ce type de services de cybersanté. En tant qu'utilisateurs des services de cybersanté centrés sur les organisations, celles-ci se concentrent essentiellement sur les fonctionnalités, le caractère modulable, la sécurité, la confidentialité et d'autres facteurs éventuels du serveur de l'application de cybersanté. Celui-ci est le composant principal des services de cybersanté centrés sur les organisations.

Services de cybersanté centrés sur la population: l'accent est mis sur la population d'une ville ou d'un pays, qui est le principal utilisateur de ce type de services de cybersanté. En tant qu'utilisateur des services de cybersanté centrés sur la population, les villes ou pays se concentrent essentiellement sur l'interopérabilité, le caractère modulable, la sécurité, la confidentialité et d'autres facteurs éventuels du serveur de l'application de cybersanté et du serveur de la plate-forme SSAS. Les serveurs des applications de cybersanté et les serveurs des plates-formes SSAS sont les composants principaux des services de cybersanté centrés sur population, comme le montre la Figure 2.

La Figure 2 illustre l'architecture d'un système de services de cybersanté faisant partie de l'IoT [UIT-T Y.4113] et de ses composants associés.

6.3 Cadre d'évaluation de la qualité de fonctionnement et avantages pour les services de cybersanté appartenant à l'IoT

L'utilisation d'une infrastructure de type IoT, c'est-à-dire d'une plate-forme SSAS centralisée, vise à rendre les systèmes de cybersanté plus efficace pour ce qui est de la prise en charge des services de cybersanté en faisant en sorte de se passer des interactions entre homologues requises dans les services de cybersanté généraux.

Toutefois, la plate-forme SSAS centralisée doit répondre aux exigences des systèmes connectés concernant l'interopérabilité, la facilité d'utilisation et la sécurité.

Il est donc nécessaire de disposer d'un cadre d'évaluation de la qualité de fonctionnement tenant compte de ces facteurs pour aider les parties prenantes des services de cybersanté appartenant à l'IoT. Ce cadre permettra de recenser les exigences des systèmes de cybersanté associés et partant, de trouver des solutions.

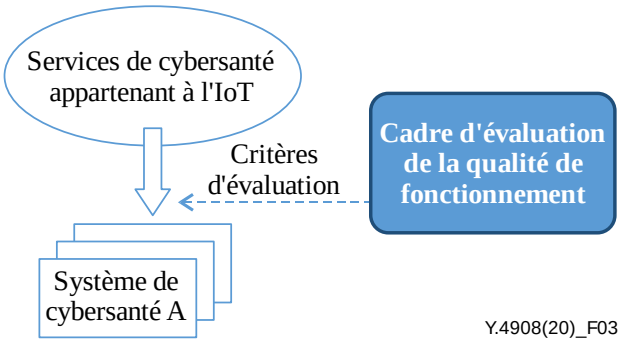

Figure 3 – Cadre d'évaluation de la qualité de fonctionnement

L'utilisation d'un cadre d'évaluation de la qualité de fonctionnement sur le modèle de la Figure 3 peut aider les parties prenantes des services de cybersanté appartenant à l'IoT:

– à mettre en place un mécanisme souple d'évaluation de l'interopérabilité lorsque plusieurs systèmes de cybersanté s'interconnectent;

– à simplifier le processus d'évaluation de la facilité d'utilisation aux fins de l'intégration verticale des systèmes de cybersanté (par exemple les systèmes des établissements de santé et les systèmes des hôpitaux) au moyen d'une plate-forme SSAS centralisée;

– à évaluer efficacement la sécurité de systèmes de cybersanté différents (par exemple les contrôles d'accès en fonction du rôle).

6.4 Parties prenantes du cadre d'évaluation de la qualité de fonctionnement

Le présent paragraphe vise à présenter les principales parties prenantes des services de cybersanté tels que décrits dans la Figure 4.

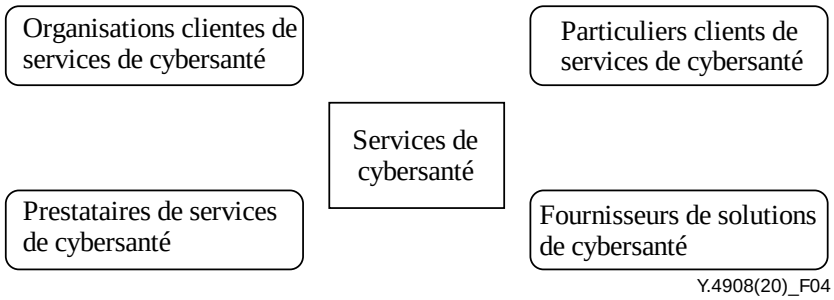

Figure 4 – Parties prenantes des services de cybersanté

Le cadre d'évaluation de la qualité de fonctionnement comprend essentiellement quatre parties prenantes, à savoir:

– les prestataires de services de cybersanté;
– les organisations clientes de services de cybersanté;
– les particuliers clients de services de cybersanté; et
– les fournisseurs de solutions de cybersanté.

7 Critères d'évaluation de la qualité de fonctionnement des systèmes de cybersanté appartenant à l'IoT

Le présent paragraphe vise à présenter trois critères non fonctionnels d'évaluation de la qualité de fonctionnement des systèmes de cybersanté appartenant à l'IoT, à savoir l'interopérabilité, la facilité d'utilisation et la sécurité.

7.1 Interopérabilité

Dans le fond, on peut faire la distinction entre l'interopérabilité des réseaux (c'est-à-dire au moyen des réseaux IoT [UIT-T Y.4113]), l'interopérabilité des données et l'interopérabilité des services (c'est-à-dire des services de cybersanté). L'interopérabilité des réseaux renvoie à la capacité des différents systèmes et dispositifs de cybersanté de s'interconnecter au niveau du réseau au moyen de la plate-forme SSAS de cybersanté. L'interopérabilité des données désigne la capacité d'échanger des données entre différents systèmes et dispositifs de cybersanté faisant partie de l'IoT. Quant à l'interopérabilité des services, il s'agit de la capacité d'intégrer sans heurts des services de cybersanté dans différents systèmes et dispositifs de cybersanté appartenant à l'IoT.

Le concept d'interopérabilité des systèmes de cybersanté présente des avantages pour les particuliers clients de services de cybersanté et les organisations clientes de services de cybersanté car, s'il est bien mis en œuvre, il devrait induire une baisse des coûts et une amélioration de la qualité de service pour les clients (par exemple, les mêmes dispositifs de cybersanté peuvent prendre en charge différents services de cybersanté).

Les prestataires de services de cybersanté et les fournisseurs de solutions de cybersanté doivent envisager d'appliquer, le cas échéant, les normes d'interopérabilité utilisées dans le secteur au lieu de leurs propres normes.

7.2 Facilité d'utilisation

Il existe un grand nombre de systèmes de cybersanté. La plupart de ces systèmes doivent trouver un moyen de répondre efficacement aux exigences des parties prenantes, qui ne cessent de changer [b-Improving Care]. Dans le cas des services de cybersanté appartenant à l'IoT (dont la plate-forme SSAS est l'infrastructure centrale), la notion de facilité d'utilisation consiste tout particulièrement à connecter efficacement les systèmes de cybersanté à la plate-forme SSAS et à répondre efficacement aux attentes des parties prenantes, qui évoluent.

Dans le cas des particuliers clients de services de cybersanté, la notion de facilité d'utilisation consiste à envoyer leurs données physiologiques et leurs informations personnelles de santé aux systèmes de cybersanté de façon pratique, et à partager ces données et informations dans le système de cybersanté lorsque l'intéressé y consent.

Dans le cas des organisations clientes de services de cybersanté, la notion de facilité d'utilisation consiste à échanger des données de cybersanté avec d'autres organisations clientes de services de cybersanté, à réutiliser les données de cybersanté, à faciliter les soins de groupe et à favoriser la coordination des soins.

Dans le cas des prestataires de services de cybersanté, la notion de facilité d'utilisation consiste à faire en sorte que les systèmes de cybersanté favorisent la coordination des soins spécialisés. La

coordination des spécialistes peut permettre à ces prestataires de rapidement soumettre leurs contributions sur la conception des systèmes de cybersanté et leurs observations concernant l'étape qui suit la mise en œuvre.

Dans le cas des fournisseurs de solutions de cybersanté, la notion de facilité d'utilisation consiste à faire en sorte que les composants des systèmes de cybersanté soient modulables et configurables, afin que les solutions de cybersanté puissent être déployées dans de nombreux scénarios différents.

7.3 Sécurité

La sécurité est un enjeu essentiel des systèmes de cybersanté, notamment lorsqu'ils appartiennent à l'IoT. Étant donné que les systèmes et dispositifs de cybersanté faisant partie de l'IoT sont connectés au moyen d'une plate-forme SSAS et n'échangent pas de données directement, ils devraient appliquer des mesures de sécurité adaptées pour fonctionner de façon sûre. Ces mesures de sécurité visent à garantir la confidentialité, l'intégrité et la disponibilité des données et services de cybersanté.

8 Cadres d'évaluation de la qualité de fonctionnement

Le présent paragraphe vise à mettre en place des cadres d'évaluation de la qualité de fonctionnement des systèmes de cybersanté appartenant à l'IoT compte tenu des trois critères définis ci-dessus, à savoir l'interopérabilité, la facilité d'utilisation et la sécurité. Ces trois critères non fonctionnels d'évaluation de la qualité de fonctionnement ne sont pas exhaustifs. En outre, il est possible d'utiliser un ou plusieurs de ces critères pour créer un cadre d'évaluation de la qualité de fonctionnement propre à un scénario de cybersanté donné lié à l'IoT.

8.1 Évaluation de l'interopérabilité

Dans le cas des services de cybersanté généraux, les interactions entre deux systèmes de cybersanté peuvent avoir lieu directement si elles suivent des normes d'interopérabilité technique communes (par exemple si elles utilisent les mêmes interfaces, les mêmes formats de données ayant une sémantique de données cohérente et les mêmes fonctionnalités) et si elles ont des paramètres de réseau communs, des flux de service communs et des règles d'administration et de sécurité communes (par exemple, le système de cybersanté A est capable de lire les informations du patient contenues dans le système de cybersanté B).

Dans le cas des services de cybersanté appartenant à l'IoT, pour résoudre les problèmes d'hétérogénéité, chaque système de cybersanté peut veiller à son interopérabilité grâce à une couche SSAS, définie dans la Recommandation [UIT-T Y.4000], qui permet de rendre compatibles les formats de données et les flux de services et donc d'assurer l'interopérabilité des services. De plus, la couche réseau garantit l'interopérabilité des réseaux, et les dispositifs de cybersanté sont connectés aux systèmes de cybersanté appartenant à l'IoT conformément aux normes [UIT-T Y.4110] et [UIT-T Y.4408], comme illustré dans la Figure 5.

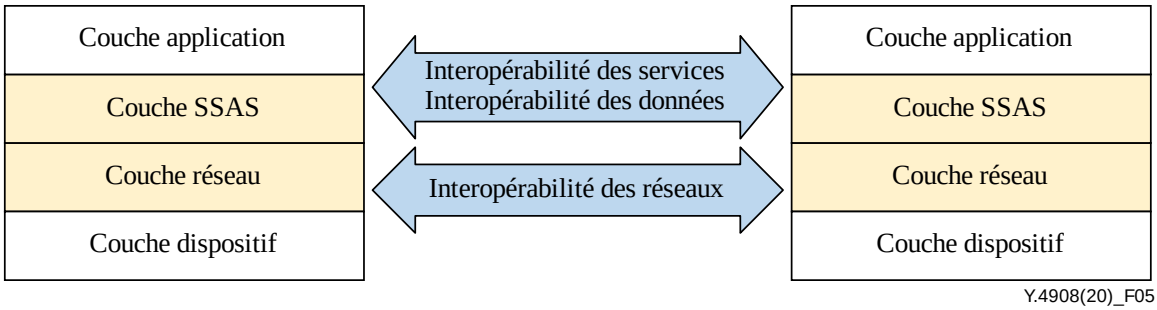

Figure 5 – Interopérabilité des systèmes de cybersanté appartenant à l'IoT grâce à la couche SSAS et à la couche réseau

L'interopérabilité des réseaux, l'interopérabilité des données et l'interopérabilité des services dont il est question dans le présent paragraphe sont trois aspects essentiels de l'évaluation de l'interopérabilité des systèmes de cybersanté appartenant à l'IoT.

8.1.1 Évaluation de l'interopérabilité des réseaux

Afin de garantir l'interopérabilité des réseaux parmi les dispositifs et les systèmes de cybersanté, les dispositifs de cybersanté devraient répondre aux exigences générales suivantes:

– Les dispositifs de cybersanté doivent prendre en charge tous les protocoles réseau requis.

– Les dispositifs de cybersanté peuvent également être connectés à une ou des passerelle(s) de cybersanté, qui permettent de convertir les protocoles réseau et d'assurer l'interfonctionnement des réseaux.

Les dispositifs de cybersanté doivent placer des données et des informations dans le cache lorsque le réseau n'est pas disponible (par exemple lorsque la connexion réseau est temporairement interrompue) et, une fois le réseau disponible, le contenu placé dans le cache peut être de nouveau synchronisé avec les systèmes de cybersanté. Les dispositifs de cybersanté doivent donc répondre aux exigences générales suivantes:

– Les dispositifs de cybersanté doivent être dotés d'un mécanisme permettant de placer des données et des informations dans un cache, afin de faire face à d'éventuelles pannes temporaires du réseau.

– Les dispositifs de cybersanté peuvent être dotés d'un mécanisme permettant de fournir des services de soins de santé essentiels lorsque le réseau est temporairement indisponible.

8.1.2 Évaluation de l'interopérabilité des données

Dans le cas de l'IoT, l'interopérabilité est une considération importante étant donné que différents types de systèmes de cybersanté s'échangent les ensembles de données produits par les dispositifs de l'IoT. Pour ce qui est des scénarios de cybersanté liés à l'IoT, chaque prestataire/partie prenante des services de cybersanté détient une partie des informations personnelles et des ensembles de données pertinents. C'est pourquoi les prestataires de services de cybersanté voudront peut-être regrouper différents ensembles de données se rapportant à une personne et stockées dans différents systèmes de cybersanté.

Par conséquent, pour fournir une analyse complète des données de cybersanté aux utilisateurs, les systèmes de cybersanté devraient répondre aux exigences générales suivantes:

– Les systèmes de cybersanté doivent prendre en charge tous les protocoles d'application requis.

– Les systèmes de cybersanté doivent avoir des interactions avec d'autres systèmes de cybersanté (par exemple les systèmes ayant des sources de données et des schémas différents).

L'interopérabilité des données suppose de tenir compte également des formats de données. La difficulté qui se pose en ce qui concerne l'interopérabilité des formats de données tient à la non-concordance des formats de protocole. Idéalement, le format de données du système de cybersanté source devrait être complètement accepté par le système de cybersanté cible. Toutefois, quand le format de données des deux systèmes ne correspond pas, les systèmes de cybersanté devraient répondre aux exigences générales suivantes:

– Les systèmes de cybersanté doivent être dotés d'un mécanisme de mise en correspondance de la syntaxe (par exemple syntaxe JSON, syntaxe XML) et de la sémantique.

– Si la syntaxe des données faisant l'objet de l'interaction entre les systèmes de cybersanté diffère, les formats de données doivent être modifiés à l'aide d'outils, afin que les données et informations échangées soient compatibles.

8.1.3 Évaluation de l'interopérabilité des services

L'interopérabilité des services consiste à faire en sorte que les applications prises en charge par deux systèmes de cybersanté puissent collaborer pour fournir des services de soins de santé aux utilisateurs finals. Il existe en général deux moyens pour assurer l'interopérabilité des services des systèmes de cybersanté faisant partie de l'IoT, soit par une association des interfaces API, soit par le portage de fonctionnalités (par exemple le portage des programmes d'application).

Concernant l'association des interfaces API, deux approches différentes peuvent être utilisées pour garantir l'interopérabilité des services:

– l'une consiste à utiliser les mêmes interfaces standard pour les systèmes de cybersanté concernés, ce qui permet aux deux systèmes d'interagir directement;

– l'autre revient à associer les interfaces dans une couche API commune (par exemple grâce aux normes sur les interfaces API ouvertes fournies par des tiers de confiance) pour résoudre les problèmes d'hétérogénéité.

En outre, la couche API commune devrait garantir une compatibilité aval pour éviter les dysfonctionnements lors des mises à niveau et des mises à jour.

À défaut, le portage de fonctionnalités consiste à déplacer une application ou ses composants d'un système de cybersanté source vers un système de cybersanté cible et à exécuter cette application dans ce dernier.

8.2 Évaluation de la facilité d'utilisation

8.2.1 Évaluation de la facilité d'utilisation des services

En général, la facilité d'utilisation des services de cybersanté peut être évaluée en définissant un ensemble de principes relatifs à la conception. Étant donné que les systèmes de cybersanté appartenant à l'IoT peuvent être utilisés dans différents scénarios verticaux, les services de cybersanté peuvent être déployés par étapes. Dans ce cas, ils peuvent être décomposés en un ensemble de sous-services, dont chacun peut être mis en œuvre en combinant diverses fonctions essentielles du système de cybersanté.

8.2.2 Évaluation de la facilité d'utilisation des données

La facilité d'utilisation des données suppose que les données de cybersanté soient naturellement exprimées de façon à anticiper les attentes des utilisateurs finals et leurs connaissances préalables.

Il est utile de veiller à ce que la "terminologie", les "icônes", la "cohérence des fonctions" et la "représentation logique" aident l'utilisateur à mieux comprendre les systèmes de cybersanté interconnectés appartenant à l'IoT.

8.2.3 Évaluation de la facilité d'utilisation du système

L'évaluation de la facilité d'utilisation du système de cybersanté vise à aider les fournisseurs de solutions de cybersanté et les prestataires de services de cybersanté à cerner les problèmes liés aux fonctionnalités et à la fiabilité du système tout en accédant aux services de différents systèmes de cybersanté.

L'utilisation sera d'autant plus facile que les services et les données de cybersanté des différents systèmes de cybersanté fonctionneront sans problème et de manière uniforme, ce qui garantira une expérience d'utilisateur homogène, en particulier lorsque les utilisateurs d'un système de cybersanté vertical devront utiliser une ou plusieurs fonctions d'un autre système vertical.

8.3 Évaluation de la sécurité

Dans la présente Recommandation, la notion de sécurité fait référence au maintien de la confidentialité, de l'intégrité et de la disponibilité des services et données de cybersanté faisant partie de l'IoT.

L'échange de données de cybersanté dans le cadre de l'IoT devrait suivre le principe de réduction des données. C'est-à-dire que seules les données de cybersanté nécessaires peuvent être consultées pour limiter les risques de fuite de données pendant l'échange.

– Confidentialité

  Dans la présente Recommandation, la notion de confidentialité consiste à protéger les données de cybersanté appartenant à l'IoT contre les accès non autorisés. Pour ce faire, on pourra notamment chiffrer les données, mettre en place un système d'authentification, contrôler les accès et garantir la sécurité des communications pour chaque système vertical et chaque plate-forme SSAS des systèmes de cybersanté appartenant à l'IoT.

  L'évaluation de la confidentialité vise à déterminer la mesure dans laquelle les systèmes de cybersanté appartenant à l'IoT mettent en œuvre ces mécanismes.

– Intégrité

  Dans la présente Recommandation, la notion d'intégrité consiste à protéger les données de cybersanté faisant partie de l'IoT contre les modifications non autorisées ou toute autre altération pendant leur transmission, leur stockage et leur traitement. Pour ce faire, on pourra mettre en place des méthodes rigoureuses de vérification de l'intégrité des données et d'autres mécanismes applicables aux systèmes de cybersanté appartenant à l'IoT.

  L'évaluation de l'intégrité vise à déterminer la mesure dans laquelle les systèmes de cybersanté appartenant à l'IoT mettent en œuvre ces méthodes et mécanismes.

– Disponibilité

  Dans la présente Recommandation, la notion de disponibilité consiste à faire en sorte que les utilisateurs autorisés aient accès aux services et données de cybersanté appartenant à l'IoT voulus en fonction des besoins. Pour ce faire, on pourra mettre en place des garanties de niveau de service et de données (par exemple des accords de niveau de service), des mécanismes de restauration et de récupération en cas de panne (par exemple en cas de panne imprévue causée par une catastrophe, une menace ou une vulnérabilité).

  L'évaluation de la disponibilité vise à déterminer la mesure dans laquelle les systèmes de cybersanté appartenant à l'IoT mettent en œuvre ces mécanismes.

Bibliographie

[b-Improving Care] American Medical Association (2014), *Improving Care: Priorities to Improve Electronic Health Record Usability*.

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