

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.2061

(06/2012)

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

Réseaux de prochaine génération – Cadre général et
modèles architecturaux fonctionnels

**Exigences relatives à la prise en charge des
applications de communication orientée
machine dans l'environnement des réseaux de
prochaine génération**

Recommandation UIT-T Y.2061

RECOMMANDATIONS UIT-T DE LA SÉRIE Y
**INFRASTRUCTURE MONDIALE DE L'INFORMATION, PROTOCOLE INTERNET ET RÉSEAUX DE
PROCHAINE GÉNÉRATION**

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

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

Recommandation UIT-T Y.2061

Exigences relatives à la prise en charge des applications de communication orientée machine dans l'environnement des réseaux de prochaine génération

Résumé

La Recommandation UIT-T Y.2061 présente un aperçu des applications de communication orientée machine (MOC) dans l'environnement des réseaux de prochaine génération (NGN). Elle décrit un écosystème MOC ainsi que les caractéristiques des communications MOC, et présente certains cas d'utilisation pertinents. A partir d'une analyse des exigences de service des applications MOC, elle définit les exigences relatives aux capacités NGN et les exigences relatives aux capacités dans le domaine de dispositifs MOC. La présente Recommandation décrit en outre un cadre de référence pour les capacités MOC.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.2061	2012-06-15	13	11.1002/1000/11560

Mots clés

Communication orientée machine (MOC), applications MOC, capacités MOC, dispositif MOC, domaine de dispositifs MOC, passerelle MOC, domaine de services MOC, réseau NGN, capacités NGN, domaine NGN, exigences de service

* 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 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/>.

© UIT 2016

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, par quelque procédé que ce soit, sans l'accord écrit préalable de l'UIT.

TABLE DES MATIÈRES

	Page
1	Domaine d'application 1
2	Références..... 1
3	Définitions 2
3.1	Termes définis ailleurs 2
3.2	Termes définis dans la présente Recommandation 2
4	Abréviations et acronymes 4
5	Conventions 4
6	Introduction..... 5
6.1	Vue d'ensemble du réseau 5
6.2	Types de communications orientées machine 6
6.3	Ecosystème MOC..... 7
7	Caractéristiques des communications MOC..... 9
8	Exigences de service des applications MOC 10
8.1	Niveaux de mobilité 10
8.2	Communications de réseau temporisées..... 10
8.3	Utilisation des ressources 10
8.4	Interopérabilité avec les dispositifs propriétaires 10
8.5	Collaboration d'applications 11
8.6	Prise en charge d'un environnement d'intégration et de fourniture de services 11
8.7	Equilibrage de la charge et robustesse..... 11
8.8	Comptabilité et taxation 12
8.9	Gestion..... 12
8.10	Adressage et identification 13
8.11	Prise en charge basée sur la localisation..... 14
8.12	Prise en charge basée sur les groupes 14
8.13	Qualité de service 15
8.14	Sécurité 16
8.15	Association et interaction des dispositifs avec des applications multiples.... 17
8.16	Communication avec les dispositifs en mode veille..... 17
8.17	Différenciation et traitement des données collectées 17
9	Exigences des capacités NGN 18
9.1	Exigences relatives aux extensions et aux adjonctions des capacités NGN... 18
9.2	Exigences prises en charge par les capacités NGN existantes 21
10	Exigences de capacité d'un domaine de dispositifs MOC 22
10.1	Mise à disposition de capacités pour les applications 22
10.2	Mobilité 22
10.3	Communication 22

	Page
10.4	Qualité de service 23
10.5	Gestion à distance 23
10.6	Adressage et identification des dispositifs 24
10.7	Sécurité 24
10.8	Comptabilité et taxation 24
10.9	Identification des données 24
11	Cadre de référence pour les capacités MOC 24
11.1	Vue de haut niveau 24
11.2	Capacités MOC dans le domaine NGN 25
11.3	Capacités MOC dans le domaine de dispositifs MOC 28
11.4	Interfaces de service MOC 29
12	Considérations relatives à la sécurité 30
	Appendice I – Acteurs et rôles associés dans l'écosystème MOC 31
	Appendice II – Cas d'utilisation des communications MOC 32
II.1	Cybersanté 32
II.2	Service d'alerte aux tsunamis 34
II.3	Gestion d'une flotte de véhicules 35
II.4	La maison intelligente 36
II.5	Intégration avec les services Internet 37
	Bibliographie 39

Recommandation UIT-T Y.2061

Exigences relatives à la prise en charge des applications de communication orientée machine dans l'environnement des réseaux de prochaine génération

1 Domaine d'application

La présente Recommandation décrit les extensions et les adjonctions des réseaux de prochaine génération ainsi que les capacités des dispositifs qui sont nécessaires à la prise en charge des applications de communication orientée machine (MOC) dans l'environnement des réseaux de prochaine génération (NGN). Bien que la présente Recommandation traite de la prise en charge des applications MOC dans l'environnement NGN, ces capacités sont conceptuellement applicables à d'autres réseaux.

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

- vue d'ensemble du réseau; description d'un écosystème MOC et des caractéristiques des communications MOC;
- exigences de service relatives à la prise en charge des applications MOC;
- exigences des capacités NGN, compte tenu des exigences de service des applications MOC;
- exigences des capacités dans le domaine de dispositifs MOC, compte tenu des exigences de service des applications MOC;
- cadre de référence pour les capacités MOC.

NOTE – L'Appendice I fournit des précisions concernant les acteurs et les rôles d'un écosystème MOC, et l'Appendice II présente des cas d'utilisation pertinents des applications MOC dans l'environnement NGN.

2 Références

La présente Recommandation se réfère à certaines dispositions des Recommandations UIT-T et textes suivants qui, de ce fait, en sont partie intégrante. Les versions indiquées étaient en vigueur au moment de la publication de la présente Recommandation. Toute Recommandation ou tout texte étant sujet à révision, les utilisateurs de la présente Recommandation sont invités à se reporter, si possible, aux versions les plus récentes des références normatives suivantes. 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 Q.1706] Recommandation UIT-T Q.1706/Y.2801 (2006), *Prescriptions de gestion de la mobilité pour les réseaux de prochaine génération.*
- [UIT-T Y.2012] Recommandation UIT-T Y.2012 (2010), *Prescriptions et architecture fonctionnelles du réseau de prochaine génération.*
- [UIT-T Y.2060] Recommandation UIT-T Y.2060 (2012), *Présentation générale de l'Internet des objets.*
- [UIT-T Y.2201] Recommandation UIT-T Y.2201 (2009), *Spécifications et capacités des réseaux de prochaine génération de l'UIT-T.*
- [UIT-T Y.2221] Recommandation UIT-T Y.2221 (2010), *Prescriptions de prise en charge pour les applications et services de réseaux de capteurs ubiquitaires dans l'environnement des réseaux de prochaine génération.*

- [UIT-T Y.2233] Recommandation UIT-T Y.2233 (2008), *Prescriptions et cadre général d'offre des capacités de comptabilité et de taxation dans les réseaux de prochaine génération.*
- [UIT-T Y.2240] Recommandation UIT-T Y.2240 (2011), *Spécifications et capacités de l'environnement d'intégration et de fourniture de services de réseau de prochaine génération.*
- [UIT-T Y.2701] Recommandation UIT-T Y.2701 (2007), *Prescriptions de sécurité des réseaux de prochaine génération de version 1.*
- [UIT-T Y.2702] Recommandation UIT-T Y.2702 (2008), *Spécifications d'authentification et d'autorisation pour les réseaux de prochaine génération de version 1.*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 dispositif [UIT-T Y.2060]: 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 passerelle [UIT-T Y.2091]: Dispositif qui interconnecte différents réseaux et qui procède à la traduction nécessaire entre les protocoles utilisés dans ces réseaux.

3.1.3 terminal d'identification [b-UIT-T Y.2213]: Dispositif capable de lire des données et, éventuellement, d'écrire des données, qui lit (et éventuellement écrit) un ou des identificateurs et, éventuellement, des données d'application à partir d'une étiquette d'identification/dans une étiquette d'identification.

3.1.4 mobilité du réseau [UIT-T Q.1703]: Capacité d'un réseau, où un ensemble de noeuds fixes ou mobiles sont reliés en réseau, de changer, comme un tout, son point de rattachement au réseau correspondant selon le déplacement du réseau lui-même.

3.1.5 environnement d'intégration et de fourniture de services NGN (NGN-SIDE) [UIT-T Y.2240]: Environnement ouvert dans le réseau NGN, qui intègre des ressources à partir de différents domaines et fournit des services intégrés aux applications sur le réseau NGN.

NOTE – Ces domaines comprennent, sans toutefois s'y limiter, un domaine de télécommunication (par exemple, réseaux fixes et mobiles), un domaine Internet, un domaine de radiodiffusion et un domaine de fournisseur de contenus.

3.1.6 capacités d'environnement de service ouvert [UIT-T Y.2234]: Capacités fournies par un environnement de service ouvert devant servir à créer et à fournir des services souples et évolués à partir de l'utilisation d'interfaces normalisées.

3.1.7 capteur [UIT-T Y.2221]: Dispositif électronique qui détecte une condition physique ou un composé chimique et fournit un signal électronique proportionnel à la caractéristique observée.

3.1.8 carte à circuit intégré universelle (UICC) [b-UIT-T Q.1741.7]: Dispositif physiquement sécurisé, carte à circuit intégré (ou carte intelligente), qui peut être inséré dans un terminal et en être retiré. La carte UICC peut contenir une ou plusieurs applications. Une des applications peut être un module USIM.

3.2 Termes définis dans la présente Recommandation

Les termes suivants sont définis ou utilisés dans la présente Recommandation:

3.2.1 actionneur: Dispositif qui accomplit des actions physiques en réaction à un signal d'entrée.

NOTE – Un actionneur pourrait, par exemple, agir sur l'écoulement d'un gaz ou d'un liquide, sur la distribution de l'électricité, ou par une opération mécanique. Les variateurs et les relais sont des exemples d'actionneurs. La décision d'activer l'actionneur peut provenir d'une application MOC, d'un être humain ou de dispositifs et de passerelles MOC.

3.2.2 communication orientée machine (MOC): Forme de communication de données entre deux entités ou plus, dans laquelle au moins une entité n'a pas nécessairement besoin d'une interaction ou d'une intervention humaine au cours de la communication.

3.2.3 capacités de communication orientée machine (MOC): Ensemble de fonctions destinées à la prise en charge et à la gestion des applications MOC, partagées par différentes applications MOC et accessibles par l'intermédiaire d'un ensemble d'interfaces normalisées.

NOTE 1 – Lorsque les capacités MOC sont prises en charge par le réseau NGN, elles fournissent des interfaces normalisées pour les applications MOC aux dispositifs et aux passerelles MOC, aux fins de la collecte, de la gestion et de l'exploitation des données. En outre, elles réutilisent les capacités NGN définies dans [UIT-T Y.2201] et [UIT-T Y.2240], les capacités informatiques ou les capacités Internet, ou interagissent avec ces capacités, afin de fournir des applications MOC.

NOTE 2 – Lorsque les capacités MOC sont prises en charge par les dispositifs et les passerelles MOC, elles interagissent avec les fonctionnalités NGN et les applications MOC par l'intermédiaire d'un ensemble d'interfaces normalisées.

3.2.4 dispositif de communication orientée machine (MOC): Dispositif qui intervient dans la prise en charge des applications MOC.

NOTE – Dans l'environnement NGN, un dispositif MOC se connecte au réseau NGN directement ou indirectement par l'intermédiaire d'une passerelle MOC.

3.2.5 utilisateur final de communication orientée machine (MOC): Utilisateur final d'applications MOC.

NOTE – Cet utilisateur peut être un système (par exemple, serveur d'application MOC, autre équipement de réseau, autres applications, dispositif MOC, passerelle MOC) ou un être humain (par exemple, utilisateur final de réseau NGN).

3.2.6 passerelle de communication orientée machine (MOC): Passerelle qui assure l'interconnexion et l'interopérabilité entre des réseaux MOC locaux et le réseau, ainsi que, le cas échéant, l'interopérabilité au niveau des applications MOC.

NOTE – Dans l'environnement NGN, une passerelle MOC joue un rôle de procuration ou d'agrégateur de données afin d'assurer l'interopérabilité et l'interconnexion entre les dispositifs MOC et le réseau NGN.

3.2.7 groupe de communication orientée machine (MOC): Liste de dispositifs et/ou de passerelles MOC regroupés selon un ou plusieurs critères.

NOTE – Les critères peuvent être l'abonné à l'application MOC, le fabricant de dispositifs MOC, l'application MOC, ou la localisation.

3.2.8 réseau local de communication orientée machine (MOC): Réseau qui assure une connectivité entre des dispositifs MOC sans l'intervention d'une passerelle MOC, ainsi qu'entre des dispositifs et des passerelles MOC.

NOTE – Un réseau MOC local peut assurer une connectivité IP et/ou non IP.

3.2.9 compteur: Dispositif qui mesure et, éventuellement, enregistre la quantité, le niveau ou le débit de quelque chose, notamment la quantité d'électricité, de gaz ou d'eau utilisée.

NOTE – Un compteur doit mesurer la consommation totale de quelque chose pendant une certaine période.

4 Abréviations et acronymes

Les abréviations et acronymes suivants sont utilisés dans la présente Recommandation.

ACI	Interface application-capacités (<i>application to capability interface</i>)
ANI	Interface application-réseau (<i>application to network interface</i>)
API	Interface de programmation d'application (<i>application programming interface</i>)
B2C	Commerce électronique de détail (<i>business to customer</i>)
CDR	Relevé de données de taxation (<i>charging data record</i>)
GNSS	Systèmes mondiaux de navigation par satellite (<i>global navigation satellite systems</i>)
GPS	Système mondial de positionnement (<i>global positioning system</i>)
IC	Circuit intégré (<i>integrated circuit</i>)
ID	Identification (<i>identification</i>)
IP	Protocole Internet (<i>internet protocol</i>)
IT	Technologies de l'information (<i>information technology</i>)
MOC	Communication orientée machine (<i>machine-oriented communication</i>)
NGN	Réseau de prochaine génération (<i>next generation network</i>)
NNI	Interface réseau-réseau (<i>network to network interface</i>)
OSE	Environnement de service ouvert (<i>open service environment</i>)
QoS	Qualité de service (<i>quality of service</i>)
SIDE	Environnement d'intégration et de fourniture de services (<i>service integration and delivery environment</i>)
SIP	Protocole d'ouverture de session (<i>session initiation protocol</i>)
SLA	Accord de niveau de service (<i>service level agreement</i>)
SMS	Service de messages courts (<i>short message service</i>)
SNS	Services de réseau social (<i>social network services</i>)
UICC	Carte à circuit intégré universelle (<i>universal integrated circuit card</i>)
UNI	Interface utilisateur-réseau (<i>user to network interface</i>)

5 Conventions

Dans la présente Recommandation:

L'expression "il est exigé" indique une exigence qui doit être strictement suivie et par rapport à laquelle aucun écart n'est permis pour pouvoir déclarer la conformité au présent document.

L'expression "il est recommandé" indique une exigence qui est recommandée mais qui n'est pas absolument nécessaire. Cette disposition n'est donc pas indispensable pour déclarer la conformité.

Les expressions "peut, à titre d'option" et "peut" indiquent une exigence optionnelle qui est admissible, sans pour autant être en quoi que ce soit recommandée. Elles ne doivent pas être interprétées comme l'obligation pour le fabricant de mettre en œuvre l'option et la possibilité pour l'opérateur de réseau ou le fournisseur de services 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.

6 Introduction

6.1 Vue d'ensemble du réseau

Les communications orientées machine (MOC) sont une forme de communication de données entre deux entités ou plus, dans laquelle au moins une entité n'a pas nécessairement besoin d'une interaction ou d'une intervention humaine au cours de la communication.

Les communications MOC permettent de communiquer avec des dispositifs MOC distants afin de réaliser des procédures telles que l'inscription, l'authentification, l'autorisation, la surveillance, la maintenance, l'approvisionnement, et la résolution des problèmes. Les applications MOC visent à automatiser les processus de décision et de communication.

La Figure 6-1 présente la vue d'ensemble du réseau pour la prise en charge des applications MOC dans l'environnement NGN.

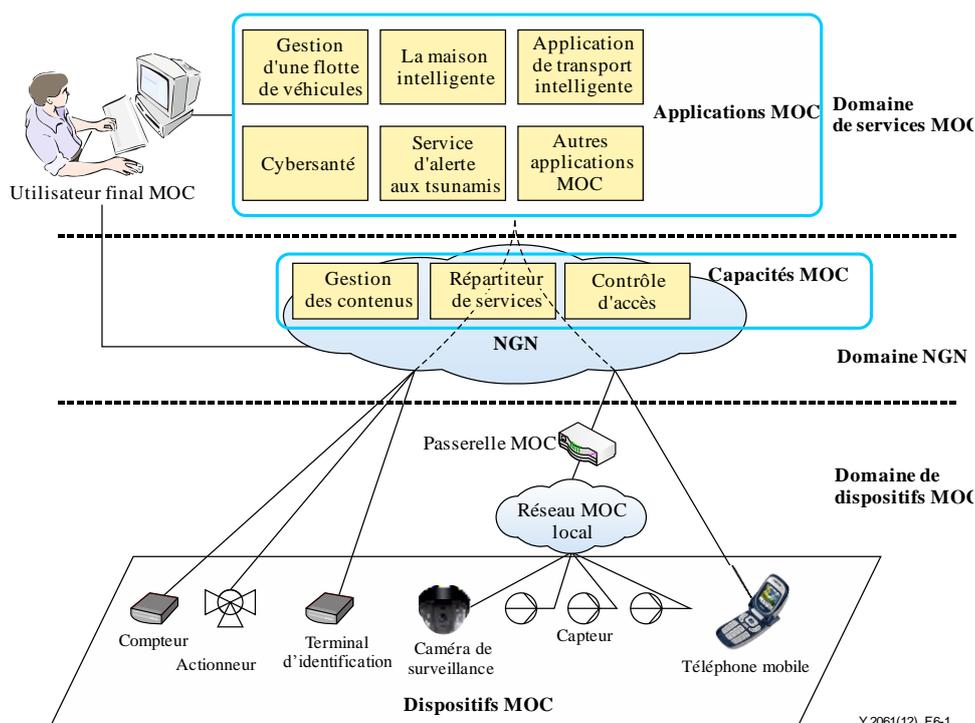


Figure 6-1 – Vue d'ensemble du réseau pour la prise en charge des applications MOC dans l'environnement NGN

Le domaine de dispositifs MOC contient des dispositifs MOC et des passerelles MOC. Les dispositifs MOC comprennent différents types de dispositifs, comme indiqué dans la Figure 6-1.

NOTE 1 – Les dispositifs propriétaires (voir la Figure 11-1) ne sont pas représentés dans la figure précédente.

On peut classer les dispositifs MOC dans les catégories suivantes: dispositifs généraux, dispositifs de saisie de données, dispositifs de transport de données et dispositifs de détection ou d'actionnement (voir [UIT-T Y.2060]). On peut citer les exemples suivants pour les différentes catégories:

- dispositifs de détection ou d'actionnement: capteurs, caméras de surveillance, compteurs, actionneurs à télécommande;
- dispositifs de saisie de données et de transport de données: terminaux d'identification;
- dispositifs généraux: téléphones mobiles, ordinateurs personnels, télévision en réseau.

Les dispositifs MOC peuvent accéder au réseau NGN directement ou par l'intermédiaire d'un réseau MOC local et des passerelles MOC qui y sont rattachées. Les dispositifs et les passerelles MOC peuvent accéder au réseau NGN à l'aide d'une connectivité filaire ou hertzienne.

Les dispositifs et les passerelles MOC peuvent accéder au réseau NGN par l'intermédiaire de réseaux à accès multiple, afin par exemple de garantir la fiabilité des communications.

Le domaine NGN assure non seulement des fonctions d'accès, de transport de données, de commande du réseau, et d'interconnexion (avec d'autres réseaux), mais fournit aussi des capacités MOC destinées à la prise en charge d'applications MOC multiples.

Les capacités MOC réutilisent les capacités NGN définies dans [UIT-T Y.2201] ou interagissent avec celles-ci, exposent des fonctionnalités aux applications MOC au moyen d'un ensemble d'interfaces normalisées, et facilitent le développement et le déploiement d'applications en cachant les spécificités du réseau aux applications MOC. Les capacités MOC comprennent des capacités destinées à la gestion des contenus, au répartiteur de services et au contrôle d'accès. On trouvera des informations détaillées dans la section 11.

NOTE 2 – Bien que cela n'apparaisse pas dans la Figure 6-1, les capacités MOC dans le réseau NGN peuvent aussi interagir avec d'autres applications extérieures au domaine de services MOC, par exemple des services de réseau social (SNS) ou des applications de type blog, qui peuvent mettre à disposition des informations relatives aux communications MOC, conformément aux prescriptions des consommateurs ou des applications.

Le domaine de services MOC contient les applications MOC. Les applications MOC exécutent la logique d'application et utilisent les capacités MOC accessibles par l'intermédiaire d'interfaces normalisées.

NOTE 3 – Bien que cela n'apparaisse pas dans la Figure 6-1, des capacités et des applications MOC peuvent aussi être contenues dans le domaine de dispositifs MOC.

6.2 Types de communications orientées machine

Les communications MOC permettent d'assurer des communications entre dispositifs MOC et êtres humains, c'est-à-dire, de manière plus précise:

- des communications entre différents dispositifs MOC et entre des dispositifs MOC et des applications MOC; et
- des communications entre des dispositifs MOC et d'autres dispositifs commandés par des êtres humains.

Le premier type de communications concerne la collecte de données, la gestion des dispositifs, l'exploitation des dispositifs, et d'autres fonctions de communication avec des équipements distants. Ces communications sont utilisées dans de nombreuses situations, par exemple celle où des applications MOC obtiennent les informations utiles fournies par des capteurs.

Le second type de communications peut être déclenché par des dispositifs MOC distants afin de fournir à des êtres humains, au moment opportun, des informations utiles détectées par des dispositifs MOC, ou par des êtres humains afin d'obtenir des informations utiles auprès de dispositifs distants. Ces communications interviennent dans de nombreuses situations, par exemple celle où un être humain se connecte à une caméra de surveillance installée chez lui au moyen d'un téléphone mobile.

Dans le cas où un dispositif MOC interagit avec des capacités MOC dans un domaine de réseau ou avec des applications MOC, l'exécution d'une application MOC dans un environnement NGN peut se décomposer selon les phases suivantes:

- Collecte des données: le dispositif MOC détecte, mesure et enregistre les données (par exemple, données relatives à des propriétés physiques, données multimédias, etc.). Lorsque le dispositif MOC atteint un seuil de déclenchement ou reçoit une instruction provenant des capacités MOC dans le domaine de réseau ou des applications MOC, il demande au réseau NGN de transférer les données à l'application MOC.

NOTE 1 – Le dispositif MOC applique la politique préconfigurée, qui peut être définie par les capacités MOC ou par les applications MOC. Conformément à cette politique, le dispositif MOC détecte les données, exécute la logique et déclenche la communication avec des applications MOC ou des dispositifs MOC commandés par des êtres humains, afin de transmettre les informations utiles.

- Transport des données: le réseau NGN crée un chemin de données entre le dispositif MOC et les capacités MOC. L'application MOC peut communiquer avec le dispositif MOC de manière directe (sans passerelle) sous réserve de l'autorisation des capacités MOC dans le réseau NGN: afin de gérer le dispositif MOC, l'application MOC obtient les informations d'autorisation auprès des capacités MOC, qui sont utilisées pour l'autorisation des communications sécurisées et la négociation de clé de la session.

NOTE 2 – Ce processus peut aussi être déclenché par le dispositif MOC.

- Analyse des données: l'application MOC analyse les données qu'elle reçoit du dispositif MOC. Les capacités MOC dans le réseau NGN peuvent aussi analyser les données, à partir de règles définies par les utilisateurs finals MOC.
- Fourniture de services: l'application MOC exécute la logique de service et définit la manière dont les informations doivent être publiées à l'intention des utilisateurs finals MOC (y compris des dispositifs MOC, des êtres humains et d'autres applications). La fourniture d'informations peut être "active", l'application MOC transmettant automatiquement les informations aux utilisateurs finals MOC. L'application MOC peut également transmettre les informations à la demande des utilisateurs finals MOC (fourniture d'informations "passive").

NOTE 3 – Toutes les phases précédentes ne sont pas nécessaires à l'exécution de toutes les applications MOC. Par exemple, un utilisateur final MOC peut envoyer une demande à une application MOC associée à un véhicule pour actionner le klaxon de ce véhicule lorsqu'il veut retrouver son véhicule dans une vaste zone de stationnement, et l'application MOC associée au véhicule en actionnera le klaxon après avoir reçu la demande. Dans cet exemple, la collecte des données et le transport des données du dispositif MOC (le véhicule) à l'application MOC ne sont pas exécutés.

6.3 Ecosystème MOC

La Figure 6-2 décrit les rôles opérationnels intervenant dans un écosystème MOC, ainsi que les relations entre eux.

Les rôles opérationnels définis dans la Figure 6-2 et leurs relations sont basés sur l'écosystème de l'IoT présenté dans [UIT-T Y.2060] et adaptés au contexte des communications MOC.

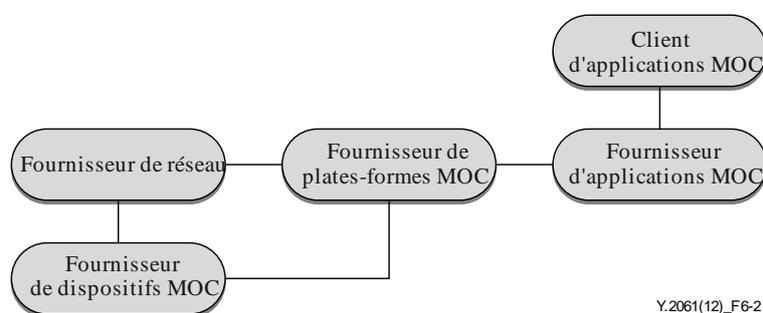


Figure 6-2 – Rôles opérationnels dans un écosystème MOC

Cinq rôles essentiels sont définis: client d'applications MOC, fournisseur de réseau, fournisseur de dispositif MOC, fournisseur de plates-formes MOC et fournisseur d'applications MOC.

- Fournisseur de réseau

Dans le contexte de la présente Recommandation, le rôle de fournisseur de réseau consiste à fournir les capacités NGN décrites dans [UIT-T Y.2201].

Le fournisseur de réseau a une relation opérationnelle avec le fournisseur de plates-formes MOC et les fournisseurs de dispositifs MOC.

NOTE 1 – Un acteur qui joue le rôle de fournisseur de réseau peut aussi jouer ceux de fournisseur de plates-formes MOC, de fournisseur de dispositifs MOC et de fournisseur d'applications MOC.

- Fournisseur d'applications MOC

Le rôle du fournisseur d'applications MOC est de fournir des fonctions dans le domaine de services MOC. Il utilise les capacités fournies par le fournisseur de plates-formes MOC afin de fournir des services au client d'applications MOC.

Le fournisseur d'applications MOC a une relation opérationnelle avec le client d'applications MOC et le fournisseur de plates-formes MOC.

NOTE 2 – Un acteur qui joue le rôle de fournisseur d'applications MOC peut aussi jouer celui de fournisseur de plates-formes MOC.

- Fournisseur de dispositifs MOC

Le fournisseur de dispositifs MOC est chargé de fournir des fonctions dans le domaine de dispositifs MOC. Il fournit des données brutes ou d'autres ressources nécessaires au fournisseur de réseau et au fournisseur de plates-formes MOC, conformément à la logique de service.

Le fournisseur de dispositifs MOC a une relation opérationnelle avec le fournisseur de plates-formes MOC et le fournisseur de réseau.

NOTE 3 – Un acteur qui joue le rôle de fournisseur de dispositifs MOC peut aussi jouer ceux de fournisseur d'applications MOC et de fournisseur de plates-formes MOC.

- Fournisseur de plates-formes MOC

Le fournisseur de plates-formes MOC est chargé de fournir les fonctions suivantes dans le domaine NGN:

- accès aux ressources mises à disposition par les fournisseurs de dispositifs MOC et le fournisseur de réseau, et intégration de ces ressources;
- prise en charge et commande des fonctionnalités d'intégration et de fourniture de services;
- fourniture de capacités (y compris l'exposition des ressources) au fournisseur d'applications MOC pour la prise en charge des applications MOC.

Le fournisseur de plates-formes MOC a une relation opérationnelle avec le fournisseur de dispositifs MOC, le fournisseur d'applications MOC et le fournisseur de réseau.

NOTE 4 – Un acteur qui joue le rôle de fournisseur de plates-formes MOC peut aussi jouer ceux de fournisseur d'applications MOC et de fournisseur de dispositifs MOC.

- Client d'applications MOC

Le client d'applications MOC peut être un être humain ou un dispositif. Il consomme les applications offertes par le fournisseur d'applications MOC. Des organismes ou des personnes, comme une entreprise, une famille ou des particuliers, sont des exemples de clients d'applications MOC.

Le client d'applications MOC a une relation opérationnelle avec le fournisseur d'applications MOC. Le client d'applications MOC est un abonné du fournisseur d'applications MOC.

NOTE 5 – Un client d'applications MOC donné peut représenter plusieurs utilisateurs finals MOC dans le domaine de services MOC.

L'Appendice I apporte des précisions concernant les acteurs et les rôles de l'écosystème MOC.

7 Caractéristiques des communications MOC

La présente section décrit les caractéristiques des communications MOC, y compris pour ce qui est des applications, des dispositifs et des passerelles. On notera que ces caractéristiques peuvent varier entre les applications, les dispositifs et les passerelles MOC. Ces caractéristiques sont présentées dans la liste suivante, qui n'est toutefois pas exhaustive:

1) Variabilité des types et des niveaux de capacité des dispositifs MOC

Il existe différents types de dispositifs MOC, destinés à différentes utilisations. Certains d'entre eux ont un niveau de performance peu élevé et une fonctionnalité limitée (par exemple, faible capacité de traitement, mémoire peu élevée, capacités de sécurité limitées), alors que d'autres possèdent de puissantes capacités intégrées (par exemple, capacités d'authentification et d'autorisation bilatérales avec le réseau et les applications MOC).

2) Prise en charge de dispositifs MOC hétérogènes par les applications MOC

Les applications MOC peuvent avoir à communiquer avec plus d'un type de dispositifs MOC. Dans ce cas, les applications MOC doivent s'adapter à cette hétérogénéité.

3) Groupement de dispositifs MOC

Dans certains cas d'utilisation, des groupes de dispositifs MOC sont déployés pour les services. En général, les dispositifs MOC d'un groupe donné ont les mêmes caractéristiques, fonctions, niveaux de performance ou politiques.

4) Variabilité des niveaux de mobilité des dispositifs et des passerelles MOC

Certains dispositifs et passerelles MOC sont mobiles et peuvent s'utiliser partout. Certains dispositifs et passerelles ne se déplacent pas. Certains dispositifs et passerelles MOC se déplacent uniquement dans une certaine zone. Certains dispositifs et passerelles MOC ne doivent pas être déplacés une fois installés (leur déplacement signifierait que ces dispositifs ont été volés).

5) Gestion à distance des dispositifs MOC lors de déploiements variés et à grande échelle

Les dispositifs MOC qui font l'objet d'un déploiement massif couvrent des zones étendues, ont une durée de vie prolongée et peuvent être "en mouvement", si bien qu'il est difficile pour les opérateurs ou les utilisateurs finals MOC de gérer tous les dispositifs sur le terrain.

La fonctionnalité de gestion à distance des dispositifs MOC (par exemple, la mise à jour des micrologiciels) est particulièrement importante dans ce type de déploiement.

6) Augmentation des menaces de sécurité du fait d'une intervention manuelle limitée

Certains dispositifs et passerelles MOC doivent être gérés à distance et non exploités manuellement sur le terrain. Il en résulte une augmentation du niveau des menaces contre la sécurité, telles que les altérations physiques, le piratage, la surveillance non autorisée, etc. Il convient par conséquent de prévoir des mesures de sécurité suffisantes pour détecter ou parer d'éventuelles attaques.

7) Variabilité des caractéristiques des communications de données

La plupart des applications MOC reposent sur des communications de données menées par des machines, sans intervention humaine. Les caractéristiques de ces communications de données sont très différentes de celles des communications menées par des êtres humains.

La diversité des communications de données est aussi liée à la variabilité d'autres facteurs, comme la taille des paquets (petits ou grands paquets), les périodes et la fréquence des transmissions de données, ou le rôle de communication des dispositifs MOC (entité d'origine ou entité de destination).

8) Grandes quantités de données transmises au réseau

Du fait de l'intelligence grandissante intégrée dans les dispositifs et du grand nombre de dispositifs connectés au réseau, de grandes quantités de données sont transmises au réseau.

8 Exigences de service des applications MOC

8.1 Niveaux de mobilité

Différents types d'applications MOC peuvent nécessiter différents niveaux de mobilité pour les dispositifs et/ou les passerelles MOC. Cette échelle de mobilité comprend l'absence de mobilité pour les dispositifs et les passerelles qui ne se déplacent pas, une mobilité limitée pour les dispositifs et les passerelles qui se déplacent de manière peu fréquente (par exemple, il est possible que des dispositifs médicaux placés sur un patient se déplacent peu souvent), ou une faible mobilité géographique pour les dispositifs et les passerelles qui se déplacent uniquement dans une certaine zone (par exemple, des dispositifs installés à bord d'un autobus, comme une caméra, peuvent ne se déplacer qu'à l'intérieur d'une ville). Il est nécessaire d'assurer une gestion de la mobilité pour différents niveaux de mobilité, afin de réduire l'utilisation des ressources (par exemple, la fréquence de la mise à jour périodique de la localisation devrait être réduite pour les dispositifs MOC qui se déplacent peu souvent).

Les exigences relatives aux niveaux de mobilité sont les suivantes:

- 1) Il est exigé que les applications MOC soient prises en charge avec une gestion optimisée de la mobilité, compte tenu des niveaux de mobilité requis.

8.2 Communications de réseau temporisées

Afin de réduire au minimum les coûts et d'optimiser l'efficacité du réseau, les dispositifs ou les passerelles MOC peuvent localement mettre en cache les données collectées et les transmettre au réseau pendant les intervalles de temps autorisés ou préconfigurés par l'opérateur de réseau.

Les exigences relatives aux communications de réseau temporisées sont les suivantes:

- 1) Il est recommandé que les applications MOC prennent en charge la temporisation des communications des dispositifs MOC avec le réseau, compte tenu des critères de service (par exemple, charge de trafic quotidienne sur le réseau, localisation des dispositifs MOC).

8.3 Utilisation des ressources

Les applications MOC sont censées utiliser peu de ressources dans le cas où les dispositifs MOC envoient ou reçoivent des données peu fréquemment (c'est-à-dire lorsqu'une longue période sépare deux transmissions de données). Afin d'améliorer l'efficacité de fonctionnement d'une application MOC et de diminuer les coûts d'exploitation de l'application MOC et la consommation d'énergie des dispositifs MOC, il est nécessaire d'optimiser l'utilisation des ressources tant par les dispositifs MOC que par les réseaux.

Les exigences des applications MOC en ce qui concerne l'utilisation optimisée des ressources sont les suivantes:

- 1) Il est recommandé que les applications MOC optimisent l'utilisation des ressources tant pour ce qui est des dispositifs MOC que des réseaux.

NOTE – Cette exigence est particulièrement importante en cas de transmissions de données peu fréquentes.

8.4 Interopérabilité avec les dispositifs propriétaires

Etant donné qu'un grand nombre de dispositifs propriétaires (par exemple, dispositifs associés à des normes propriétaires relatives à l'interfonctionnement avec des entités de réseau) ont déjà été déployés, les applications MOC devraient prendre en charge l'interopérabilité avec ces dispositifs.

Les exigences relatives à la prise en charge des dispositifs propriétaires sont les suivantes:

- 1) Il est recommandé que les applications MOC soient interopérables avec les dispositifs propriétaires grâce à l'utilisation de moyens appropriés, par exemple des passerelles MOC.
- 2) Il est recommandé que les applications MOC prennent en charge le masquage effectif des opérations des dispositifs propriétaires.

8.5 Collaboration d'applications

Dans certains cas d'applications MOC, plusieurs fournisseurs d'applications MOC peuvent fournir différentes applications MOC qui doivent collaborer entre elles.

Par exemple, les entreprises de commerce électronique grand public (B2C) fournissent des produits à des entreprises logistiques, qui sont elles-mêmes chargées de livrer ces produits aux clients qui les ont commandés. Les entreprises logistiques suivent les produits après leur expédition, et les clients peuvent suivre l'acheminement des produits qu'ils ont achetés en consultant les systèmes d'application des entreprises B2C, qui collaborent avec les systèmes d'application des entreprises logistiques.

Les exigences des applications MOC relatives à la collaboration entre applications sont les suivantes:

- 1) Il est recommandé que les applications MOC prennent en charge la collaboration avec d'autres applications MOC, par l'intermédiaire des capacités MOC.
- 2) Il est recommandé que les applications MOC d'un fournisseur d'applications MOC donné prennent en charge la collaboration avec les applications MOC d'autres fournisseurs d'applications MOC, par l'intermédiaire des capacités MOC.

8.6 Prise en charge d'un environnement d'intégration et de fourniture de services

La prise en charge par le réseau d'un environnement d'intégration et de fourniture de services aurait une incidence favorable sur les applications MOC. Outre la prise en charge de capacités générales concernant différents types d'applications, les interfaces vers cet environnement permettraient la prise en charge de capacités propres aux applications MOC.

Les exigences des applications MOC concernant la prise en charge d'un environnement d'intégration et de fourniture de services sont les suivantes:

- 1) Il est recommandé que les applications MOC puissent accéder à des capacités liées à un environnement d'intégration et de fourniture de services fournies par le réseau.

NOTE – L'accès à ce type d'environnement donne également accès à des capacités de développement et de test d'applications.

8.7 Equilibrage de la charge et robustesse

Dans certains cas d'applications, par exemple dans le cas d'une application de surveillance d'un fleuve où le niveau du fleuve atteint le seuil d'alerte, un grand nombre de points de contrôle peuvent envoyer des informations d'alerte aux capacités MOC dans le domaine NGN, avec notamment la possibilité d'envoyer des vidéos en temps réel. Ces situations d'urgence nécessitent une certaine robustesse du réseau et des capacités MOC dans le domaine NGN.

La distribution des dispositifs MOC entre différents territoires et la densité des dispositifs MOC dans une certaine zone peuvent être élevées ou faibles. Il peut en résulter un déséquilibre au niveau du réseau et des capacités MOC dans le domaine NGN, tant du point de vue de la signalisation que du trafic des données.

Les exigences destinées à prendre en charge l'équilibrage de la charge et la robustesse du réseau et des plates-formes MOC sont les suivantes:

- 1) Les applications MOC exigent des mécanismes dans le réseau et dans les capacités MOC dans le domaine NGN pour assurer l'équilibrage de la charge.
- 2) Les applications MOC exigent une certaine robustesse du réseau et des capacités MOC dans le domaine NGN, ainsi que la garantie d'une qualité de service suffisante dans des circonstances données, par exemple dans les situations d'urgence.

8.8 Comptabilité et taxation

Il est nécessaire de définir différentes exigences de comptabilité et de taxation, en fonction des cas d'utilisation des applications MOC. Par exemple, certaines applications MOC transmettent fréquemment des données en petites quantités; dans ce cas, la taxation et la comptabilité peuvent être basées sur le nombre de communications. D'autres applications MOC peuvent se connecter rarement au réseau, mais générer de grandes quantités de données lors de chaque communication; dans ce cas, la taxation et la comptabilité peuvent être basées sur la quantité de données. Dans d'autres cas, la taxation et la comptabilité peuvent être basées sur la durée des communications.

Dans la mesure où une application MOC peut utiliser plusieurs dispositifs pour un seul client, une taxation par dispositif de la part des fournisseurs d'applications MOC ou des fournisseurs de réseau, engendrerait une grande quantité de relevés de données de taxation (CDR, *charging data record*), ce qui ferait peser une lourde charge sur certaines fonctions, par exemple la fonction de taxation. Dans ces cas d'utilisation, il peut être plus approprié d'appliquer une comptabilité et une taxation par groupe plutôt que par dispositif.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est exigé que les applications MOC prennent en charge différentes méthodes de taxation et de comptabilité, telles que la taxation basée sur la durée des communications, sur le nombre de communications, sur la quantité de données transmises, etc.
- 2) Il est recommandé que les applications MOC prennent en charge une taxation unifiée pour les clients.
- 3) Lorsque la prise en charge basée sur les groupes est mise en œuvre (voir la section 8.12), il est exigé que les applications MOC prennent en charge une comptabilité et une taxation en ligne et hors ligne basées sur les groupes.

8.9 Gestion

8.9.1 Gestion des dispositifs

Les dispositifs MOC couvrent de vastes zones, ont une longue durée de vie et peuvent être "en mouvement", si bien qu'il peut se révéler difficile pour les opérateurs ou les abonnés de gérer ces dispositifs manuellement. Par conséquent, les dispositifs et les passerelles MOC devraient être gérés et surveillés à distance (par exemple, pour effectuer la mise à jour des micrologiciels afin de corriger des anomalies).

Les dispositifs MOC munis d'une carte à circuit intégré universelle (UICC) peuvent être déployés en extérieur sans supervision humaine, et il se pourrait qu'une carte UICC donnée soit placée dans un autre dispositif sans la permission du propriétaire de la carte UICC. Par conséquent, afin d'éviter ce type de problèmes, le changement d'association entre un dispositif MOC et une carte UICC devrait être accessible aux applications MOC qui interagissent avec ce dispositif MOC.

Lorsque les dispositifs et les passerelles MOC fournissent une logique de service, ils fournissent des capacités de prise en charge tant pour le client que pour le service. Il est exigé que les dispositifs et les passerelles MOC soient gérés tant en termes de gestion du réseau que de gestion du service.

Les exigences relatives à la gestion des dispositifs MOC sont les suivantes:

- 1) Il est exigé que les applications MOC prennent en charge des mécanismes de gestion des passerelles qui jouent le rôle d'agrégateurs de trafic (une passerelle agrège du trafic et agit comme un canal).
- 2) Il est exigé que les applications MOC surveillent l'état des dispositifs et des passerelles MOC en ce qui concerne divers aspects, à savoir:
 - a) un comportement anormal des dispositifs et des passerelles MOC, comme dans le cas où un service actif ne correspond pas à ce qui a été souscrit;

- b) l'association entre les dispositifs et les passerelles MOC et les cartes UICC;
 - c) les informations de rattachement des dispositifs et des passerelles MOC, par exemple la localisation du rattachement;
 - d) la connectivité des dispositifs et des passerelles MOC.
- 3) Il est exigé que les applications MOC prennent en charge des mécanismes qui permettent d'assurer de manière simple et évolutive la préfourriture des dispositifs et des passerelles MOC, d'activer et de désactiver des fonctionnalités, de signaler des erreurs au niveau des dispositifs et d'interroger l'état des dispositifs.
- 4) Il est exigé que les applications MOC prennent en charge des mécanismes de mise à niveau des logiciels (par exemple, fourniture d'une nouvelle logique de service et/ou de corrections d'erreur à charger sur les dispositifs et/ou les passerelles, y compris les applications et les logiciels d'exploitation).
- 5) Il est exigé que les applications MOC gèrent les dispositifs MOC de faibles capacités à l'aide de mécanismes légers.

8.9.2 Gestion des profils de service

Le profil de service d'une application MOC donnée est constitué d'un ensemble d'informations propres à cette application. Il peut comporter, sans toutefois s'y limiter, l'identifiant de l'application MOC, l'identifiant du fournisseur de l'application MOC et les types de données de l'application.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est recommandé que les applications MOC utilisent des profils de service normalisés pour l'enregistrement et la découverte.
- 2) Il est exigé que les applications MOC prennent en charge des mécanismes de mise à jour des profils de service.

8.9.3 Gestion des profils de dispositif

Le profil de dispositif MOC est un ensemble d'informations relatives aux dispositifs et aux passerelles MOC. Dans la mesure où il existe différents types de dispositifs et de passerelles MOC, les profils de dispositif MOC sont utiles lorsqu'il s'agit de gérer de grandes quantités de dispositifs et de passerelles hétérogènes.

NOTE 1 – Les informations du profil de dispositif MOC peuvent comporter l'identifiant du dispositif MOC, le type du dispositif MOC, les capacités du dispositif MOC et la localisation du dispositif MOC.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est recommandé que les applications MOC utilisent et gèrent des profils de dispositif normalisés pour les dispositifs et les passerelles MOC, y compris pour leur enregistrement et leur découverte.

NOTE 2 – La gestion des profils de dispositif comprend la création d'associations entre les dispositifs (passerelles) MOC et les profils de service.

8.10 Adressage et identification

Il existe deux types de méthodes de connexion entre les dispositifs MOC et les applications MOC. Les dispositifs MOC peuvent se connecter aux applications MOC directement ou par l'intermédiaire de passerelles MOC à l'aide de la connectivité IP. Différents dispositifs MOC peuvent communiquer avec différentes applications MOC par l'intermédiaire d'une passerelle unique ou de plusieurs passerelles.

NOTE – L'utilisation de plusieurs passerelles permet de réduire la charge des passerelles MOC et d'accroître la fiabilité de l'accès au réseau.

Les dispositifs MOC peuvent prendre en charge des adresses IP publiques ou privées et peuvent aussi prendre en charge des adresses non IP lorsqu'ils se connectent au réseau par l'intermédiaire de passerelles MOC. Les serveurs d'application MOC et les dispositifs MOC qui utilisent des adresses IP publiques devraient être capables de communiquer avec d'autres dispositifs MOC qui utilisent des adresses IP privées.

Les exigences relatives à l'adressage et à l'identification sont les suivantes:

- 1) Il est exigé que les applications MOC soient capables de fonctionner avec différents systèmes d'adressage des dispositifs MOC, par exemple des systèmes d'adressage IP et non IP.
- 2) Les applications MOC exigent la prise en charge d'une identification unique des dispositifs MOC.
- 3) Les applications MOC exigent la prise en charge d'une identification unique des groupes MOC (voir la section 8.12 pour la description d'un groupe MOC).
- 4) Les applications MOC exigent la prise en charge de mécanismes d'adressage qui permettent de communiquer avec des dispositifs MOC situés derrière une passerelle MOC.
- 5) Les applications MOC exigent la prise en charge de mécanismes d'adressage qui permettent de communiquer avec des passerelles MOC.
- 6) Les applications MOC exigent la prise en charge d'une identification unique des passerelles MOC.

8.11 Prise en charge basée sur la localisation

Les applications MOC peuvent collecter des données de localisation auprès des dispositifs et des passerelles MOC ou auprès du réseau. Les types d'informations de localisation comprennent les systèmes mondiaux de navigation par satellite (GNSS), la latitude et la longitude, ou l'identifiant de cellule (CellID).

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est exigé que les applications MOC connaissent la localisation des dispositifs MOC. Par exemple, à partir des informations de localisation des dispositifs MOC, l'application MOC pourrait lancer un déclenchement de service afin de mettre à niveau les micrologiciels sur les dispositifs MOC situés dans une certaine zone, au moyen de la radiodiffusion ou de la multidiffusion.
- 2) Il est recommandé que les applications MOC assurent la maintenance et la gestion des informations de localisation, tant pour un dispositif MOC unique que pour un groupe de dispositifs MOC situés derrière une passerelle MOC.
- 3) Il est recommandé que les applications MOC assurent la maintenance et la gestion de différents types d'informations de localisation.

8.12 Prise en charge basée sur les groupes

Les groupes MOC peuvent être utilisés dans de nombreuses applications MOC. Par exemple, le propriétaire d'une entreprise automobile pourrait gérer les véhicules de l'entreprise par groupe, par exemple en suivant la localisation de tous les véhicules du groupe et en envoyant des notifications à ces véhicules. Une entreprise d'électricité pourrait collecter les données de comptage de tous les dispositifs MOC situés dans une certaine zone à un moment donné. Un consommateur pourrait relever les différents compteurs de son domicile pendant qu'il est en voyage d'affaires.

Différentes applications MOC peuvent avoir des groupes MOC différents.

Les applications MOC peuvent avoir des groupes MOC statiques qui sont préconfigurés; par exemple, le consommateur pourrait préconfigurer les dispositifs MOC installés à son domicile pour constituer

un groupe MOC. Les applications MOC peuvent aussi avoir des groupes dynamiques, qui sont formés selon des critères à la demande; par exemple, le propriétaire d'une entreprise automobile peut, si nécessaire, demander à communiquer avec tous les véhicules se trouvant dans une certaine zone.

Les dispositifs MOC faisant partie d'un groupe peuvent se connecter directement ou indirectement au réseau.

Les exigences relatives à la prise en charge basée sur les groupes sont les suivantes:

- 1) Les applications MOC exigent la prise en charge de groupes MOC statiques et dynamiques.
- 2) Les applications MOC exigent la prise en charge des transmissions de données à destination ou en provenance d'un ou de tous les membres d'un groupe MOC à l'aide d'un identifiant de groupe.
- 3) Les applications MOC exigent la prise en charge de la politique de qualité de service basée sur les groupes.
- 4) Les applications MOC exigent la prise en charge de paramètres de trafic basés sur les groupes.
- 5) Les applications MOC exigent la prise en charge de la gestion des groupes MOC, y compris l'affichage, la création, la modification et la suppression des groupes MOC et des attributs associés, et l'affichage, l'ajout, la modification et la suppression des membres des groupes.
- 6) Il est recommandé que les applications MOC soient capables d'envoyer des données par groupe MOC et de hiérarchiser les données conformément à la hiérarchisation des données des membres du groupe MOC.

8.13 Qualité de service

8.13.1 Commande de trafic d'application

Le trafic d'application est engendré non seulement par les dispositifs MOC, mais aussi par les applications MOC.

Les applications MOC couvrent souvent un grand nombre de dispositifs et de passerelles MOC. Dans ce cas, du point de vue des applications, un trafic d'application élevé peut avoir des incidences sur la qualité de service.

Du point de vue du réseau, une bonne gestion du trafic d'application peut permettre d'améliorer la qualité de service des applications MOC.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Les applications MOC exigent des mécanismes de gestion du trafic d'application, afin par exemple de limiter le nombre maximal de transactions d'application par seconde.
- 2) Les applications MOC exigent d'éviter la concentration de l'accès dans une seule ressource.

8.13.2 Hiérarchisation des données

Les applications MOC essentielles aux missions doivent être gérées rigoureusement. Par exemple, la notification d'une situation d'urgence, telle qu'un incendie, doit être transmise dans les meilleurs délais et de manière fiable aux systèmes nationaux de surveillance des catastrophes concernés. Afin d'envoyer des notifications d'alarme, les données relatives à la situation d'urgence sont acheminées sur le réseau.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est recommandé que les applications MOC soient capables d'établir la hiérarchisation des données (au niveau d'une seule application ou entre différentes applications).

- 2) Il est recommandé que les applications MOC soient capables de gérer différentes données en fonction de leur niveau de priorité.
- 3) Il est recommandé que les applications MOC soient capables d'appliquer la hiérarchisation des données aux dispositifs et aux passerelles MOC conformément aux accords de niveau de service (SLA, *service level agreement*) applicables entre les clients d'applications MOC et les fournisseurs d'applications MOC.

8.14 Sécurité

8.14.1 Authentification et autorisation

Les utilisateurs finals MOC qui accèdent à des applications MOC doivent être authentifiés et autorisés. L'accès aux applications doit respecter les niveaux de sécurité applicables.

Les dispositifs MOC utilisés par les applications MOC et connectés directement doivent être authentifiés et autorisés.

Les dispositifs MOC utilisés par les applications MOC et connectés par l'intermédiaire d'une passerelle MOC devraient généralement être authentifiés et autorisés.

Les exigences relatives à l'authentification et à l'autorisation sont les suivantes:

- 1) Il est exigé que les applications MOC prennent en charge l'authentification et l'autorisation des utilisateurs finals MOC pour l'accès aux applications MOC et aux données associées, conformément aux niveaux de sécurité applicables.
- 2) Il est exigé que les applications MOC prennent en charge un mécanisme d'authentification et d'autorisation des dispositifs MOC directement connectés associés aux applications MOC elles-mêmes.
- 3) Il est recommandé que les applications MOC prennent en charge un mécanisme d'authentification et d'autorisation des dispositifs MOC qui font partie d'un réseau local (connectés par l'intermédiaire d'une passerelle MOC) et qui sont associés aux applications MOC elles-mêmes.
- 4) Il est exigé que les applications MOC prennent en charge un mécanisme d'enregistrement des dispositifs MOC directement connectés associés aux applications MOC elles-mêmes.

8.14.2 Sécurité des données

En général, les applications MOC exigent un niveau de sécurité élevé, en raison du caractère très sensible des données. Il faut tenir compte du fait que les dispositifs MOC ne peuvent pas fournir toutes les fonctionnalités de sécurité, étant donné qu'ils peuvent eux-mêmes présenter des limitations au niveau du système. Par exemple, les données détectées transportées sur le réseau peuvent ne pas être suffisamment protégées du point de vue de la sécurité.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est exigé que les applications MOC assurent la sécurité de la connectivité entre les applications MOC et les dispositifs MOC, et ce même lorsque les dispositifs MOC se déplacent d'un domaine de réseau à un autre domaine de réseau.
- 2) Il est exigé que les applications MOC prennent en charge l'intégrité et la confidentialité des données échangées lors de l'exploitation des applications.
- 3) Il est recommandé que les applications MOC fournissent des mécanismes de cryptage des données, afin de prendre en charge les dispositifs MOC disposant de capacités limitées.

8.14.3 Sécurité de l'accès aux dispositifs MOC

Toutes les données produites par les dispositifs MOC doivent rester inconnues des entités non autorisées. Par exemple, les données confidentielles ou sensibles d'un dispositif MOC ne devraient pas être envoyées à un utilisateur final non authentifié si celui-ci lance une communication avec le dispositif MOC.

En raison des capacités limitées des dispositifs MOC qui ne prennent pas en charge de fonctionnalités d'authentification et d'autorisation, les applications MOC sont soumises aux exigences suivantes:

- 1) Avant que les utilisateurs finals MOC et les applications MOC ne puissent utiliser les ressources des dispositifs MOC, il est exigé que les applications MOC prennent en charge des mécanismes d'authentification et d'autorisation des utilisateurs finals MOC et des applications MOC pour ce qui est de l'accès aux ressources des dispositifs MOC.

8.15 Association et interaction des dispositifs avec des applications multiples

Dans certains cas d'utilisation des applications MOC, il se peut qu'un dispositif MOC unique doive communiquer simultanément avec différentes applications MOC. Par exemple, lorsqu'un accident de la route a eu lieu, il est possible que le véhicule endommagé doive fournir des informations à la fois au centre de services de santé et à l'organisme chargé de gérer la circulation.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est exigé que les applications MOC n'empêchent pas la fourniture d'informations à d'autres applications MOC par un dispositif ou une passerelle MOC qui leur est associé.
- 2) Il est exigé que les applications MOC n'empêchent pas un dispositif ou une passerelle MOC qui leur est associé de recevoir des informations en provenance d'autres applications MOC.

NOTE – Dans la présente Recommandation, on suppose que la capacité d'un dispositif ou d'une passerelle MOC à communiquer avec des applications MOC multiples est contrôlée par le réseau (c'est-à-dire le réseau NGN). Les exigences d'un dispositif ou d'une passerelle MOC doté d'une "capacité indépendante du contrôle du réseau" à communiquer avec des applications MOC multiples doit faire l'objet d'autres études.

8.16 Communication avec les dispositifs en mode veille

Si les dispositifs MOC restent hors ligne pendant un certain temps, ils peuvent entrer ou rester en mode veille, afin:

- d'économiser de l'énergie, en particulier dans le cas des dispositifs utilisant une batterie;
- d'économiser les ressources du réseau, en particulier dans le cas des dispositifs qui accèdent au réseau par voie hertzienne.

NOTE – Le mode veille est un mode d'économie d'énergie. Il désigne normalement l'état d'un dispositif MOC dans une situation où, le trafic n'étant pas généré pendant un certain temps, les sessions des dispositifs et les voies de trafic correspondantes sont libérées afin d'économiser des ressources, et où tous les composants non nécessaires sont éteints. En fonction de certains critères, un dispositif MOC à l'état hors ligne peut entrer en mode veille.

Les applications MOC sont soumises aux exigences suivantes:

- 1) Il est recommandé que les applications MOC soient capables d'envoyer des instructions à un dispositif MOC en mode veille afin de le réveiller.
- 2) Il est exigé que les applications MOC prennent en charge les communications déclenchées par le réseau à destination d'un dispositif MOC en mode veille.

8.17 Différenciation et traitement des données collectées

Au vu de la grande diversité des données collectées par les dispositifs MOC qui sont transmises sur le réseau, celui-ci est censé être capable de différencier des données collectées particulières d'autres

données, puis de déclencher les processus appropriés compte tenu de leur catégorie. Par exemple, le réseau peut mettre en cache et ne transmettre qu'ultérieurement des données qui sont collectées dans des applications hors réseau sensibles à la performance. En revanche, le réseau doit immédiatement transmettre les données de priorité élevée qui sont collectées dans des applications en réseau sensibles à la performance.

Les exigences des applications MOC pour ce qui est de la différenciation des données collectées et du traitement associé de ces données sont les suivantes:

- 1) Il est exigé que les applications MOC permettent l'identification et la catégorisation des données collectées par les dispositifs MOC, conformément aux politiques applicables.
- 2) Si le réseau peut traiter les données collectées par les dispositifs MOC conformément à la catégorisation pertinente des données, alors il est exigé que les applications MOC gèrent ces données en conséquence.

9 Exigences des capacités NGN

9.1 Exigences relatives aux extensions et aux adjonctions des capacités NGN

L'objet de la présente section est de décrire les extensions ou adjonctions des capacités NGN définies dans [UIT-T Y.2221] pour la prise en charge des applications MOC.

9.1.1 Numérotage, nommage et adressage

Les réseaux NGN fournissent des capacités d'adressage et d'identification. Les exigences de service définies dans la section 8.10 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201] et [UIT-T Y.2702].

Compte tenu des exigences de service définies dans la section 8.12, les réseaux NGN sont soumis aux exigences supplémentaires suivantes concernant le numérotage, le nommage et l'adressage:

- 1) Il est exigé qu'un réseau NGN fournisse des mécanismes d'adressage par groupe pour la prise en charge des applications MOC conformément à la politique du fournisseur de réseau NGN.
- 2) Il est exigé qu'un réseau NGN prenne en charge une capacité de groupes MOC statiques.

NOTE 1 – Un groupe MOC statique contient les membres des dispositifs et de la passerelle MOC qui sont préconfigurés.

- 3) Il est exigé qu'un réseau NGN prenne en charge une capacité de groupes MOC dynamiques.

NOTE 2 – Un groupe MOC dynamique peut être créé sur demande en fonction de critères particuliers, tels que la localisation, l'état des dispositifs et des passerelles MOC, etc.

- 4) Il est exigé qu'un réseau NGN prenne en charge une capacité de groupes MOC, tant dans le cas où les dispositifs et les passerelles qui constituent les groupes sont connectés directement au réseau NGN que dans le cas où ils sont connectés indirectement au réseau NGN.
- 5) Il est exigé qu'un réseau NGN mette en correspondance l'identifiant de groupe MOC avec les adresses réseau des dispositifs et des passerelles MOC d'un groupe MOC statique.
- 6) Il est exigé qu'un réseau NGN détermine la liste ainsi que les adresses réseau des dispositifs et des passerelles MOC qui correspondent aux critères définis pour un groupe dynamique.

9.1.2 Qualité de service

Les exigences relatives à la qualité de service différenciée et à la hiérarchisation des données définies dans la section 8.13 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201] et [UIT-T Y.2221]. Les sous-sections suivantes définissent les exigences relatives aux extensions des réseaux NGN.

9.1.2.1 Politique de qualité de service par groupe

Compte tenu des exigences de service définies dans la section 8.12, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 1) Il est exigé qu'un réseau NGN prenne en charge une politique de qualité de service de niveau groupe, parallèlement à une politique de qualité de service de niveau dispositif, ou à la place de celle-ci.

NOTE – Les paramètres d'une politique de qualité de service par groupe comprennent, sans toutefois s'y limiter:

- le temps de transfert des paquets;
- la variation du temps de transfert des paquets;
- le taux de perte de paquets;
- le taux d'erreurs sur les paquets.

9.1.2.2 Commande du trafic

Les réseaux NGN disposent de capacités de traitement et de gestion du trafic. Les exigences de service définies dans la section 8.7 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201].

Compte tenu des exigences relatives aux communications de réseau temporisées définies dans la section 8.2, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 1) Il est exigé qu'un réseau NGN autorise l'accès des utilisateurs finals MOC (par exemple, rattachement au réseau ou établissement d'une connexion de données) pendant un intervalle de temps défini au cours duquel l'accès aux communications de réseau est autorisé.
- 2) Il est exigé qu'un réseau NGN refuse l'accès des utilisateurs finals MOC (par exemple, rattachement au réseau ou établissement d'une connexion de données), ou de l'autoriser avec des paramètres de taxation différents, pendant un intervalle de temps défini au cours duquel l'accès aux communications de réseau est interdit.
- 3) Il est exigé qu'un réseau NGN permette la modification des intervalles au cours desquels l'accès aux communications de réseau est autorisé, compte tenu des critères de service (par exemple, la charge de trafic quotidienne sur le réseau et la localisation des dispositifs MOC).
- 4) Il est exigé qu'un réseau NGN communique aux dispositifs et aux passerelles MOC l'horaire et la durée des intervalles de temps au cours desquels l'accès aux communications de réseau est autorisé.
- 5) Il est exigé qu'un réseau NGN mette fin à l'accès des utilisateurs finals MOC (par exemple, détachement du réseau ou libération d'une connexion de données) lorsque l'intervalle de temps au cours duquel l'accès aux communications de réseau est autorisé s'est écoulé.
- 6) Un réseau NGN peut, à titre d'option, prendre en charge la communication à des utilisateurs finals MOC autres que les dispositifs et les passerelles MOC (par exemple, les serveurs d'application MOC) des horaires et de la durée des intervalles de temps au cours desquels l'accès aux communications de réseau est autorisé.

Compte tenu des exigences relatives à l'utilisation des ressources définies dans les sections 8.3 et 8.16, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 7) Il est exigé qu'un réseau NGN avertisse les dispositifs et les passerelles MOC cibles avant l'interaction de service lorsque le réseau doit lancer un service.
- 8) Il est exigé qu'un réseau NGN n'établisse de ressources de communication que lorsqu'une transmission de données est nécessaire.

Compte tenu des exigences définies dans la section 8.12, outre les capacités de commande du trafic existantes des réseaux NGN, il est exigé qu'un réseau NGN prenne en charge:

- 9) un traitement optimisé des communications de groupe, afin d'économiser les ressources du réseau et d'éviter l'encombrement du réseau;
- 10) une commande du trafic de niveau groupe, parallèlement à une commande du trafic de niveau dispositif, ou à la place de celle-ci.

NOTE – Les paramètres de commande du trafic par groupe comprennent, sans toutefois s'y limiter:

- la taille de paquet maximale autorisée;
- le débit de données et la taille de seau;
- le débit maximal et taille de seau maximale;
- le débit moyen et la taille de seau moyenne.

9.1.3 Comptabilité et taxation

Compte tenu des exigences de service définies dans la section 8.8, les réseaux NGN sont soumis aux exigences suivantes, en plus de celles définies dans [UIT-T Y.2233]:

- 1) Il est exigé qu'un réseau NGN prenne en charge une comptabilité et une taxation par groupe pour la taxation en ligne et/ou hors ligne, parallèlement à une taxation par dispositif, ou à la place de celle-ci.

9.1.4 Mobilité

Les réseaux NGN prennent en charge la mobilité pour les utilisateurs finals et les dispositifs et les passerelles MOC, conformément aux dispositions de [UIT-T Y.2201] et [UIT-T Q.1706].

Compte tenu des niveaux de mobilité décrits dans la section 8.1, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 1) Il est exigé qu'un réseau NGN prenne en charge des niveaux de mobilité prédéfinis pour les dispositifs et les passerelles MOC, par l'intermédiaire de la gestion des profils de dispositif.
- 2) Il est exigé qu'un réseau NGN prenne en charge la gestion de différents niveaux de mobilité, compte tenu des exigences de mobilité des dispositifs et des passerelles MOC, en réduisant par exemple la fréquence des procédures de gestion de la mobilité pour les dispositifs et les passerelles MOC à faible mobilité.
- 3) Il est recommandé qu'un réseau NGN prenne en charge l'instruction dynamique des dispositifs et des passerelles MOC afin de définir le niveau de mobilité (ce qui implique, par exemple, l'ajustement de la fréquence des procédures de gestion de la mobilité).

9.1.5 Gestion des profils

9.1.5.1 Gestion des profils d'utilisateur

Compte tenu des exigences de service définies dans la section 8.9.2, les réseaux NGN sont soumis aux exigences suivantes:

- 1) Il est recommandé qu'un réseau NGN prenne en charge des profils de service normalisés comportant des améliorations pour les informations spécifiques aux applications MOC.

9.1.5.2 Gestion des profils de dispositif

Compte tenu des exigences de service définies dans la section 8.9.3, les réseaux NGN sont soumis aux exigences suivantes:

- 1) Il est recommandé qu'un réseau NGN prenne en charge des profils de dispositif normalisés comportant des améliorations pour les informations spécifiques aux dispositifs et aux passerelles MOC.

9.1.6 Gestion des dispositifs

Compte tenu des exigences de service définies dans la section 8.9.1, il est exigé que les réseaux NGN prennent en charge les exigences supplémentaires suivantes concernant la gestion des dispositifs:

- 1) Il est exigé qu'un réseau NGN soit capable de gérer et de commander des dispositifs et des passerelles MOC, ce qui consiste à:
 - a) surveiller l'exploitation des dispositifs et des passerelles MOC;
 - b) surveiller, le cas échéant, les modifications, ainsi que les actions correspondantes, au niveau des associations entre les dispositifs ou les passerelles MOC et les cartes UICC;
 - c) surveiller les modifications, ainsi que les actions correspondantes, concernant les points de rattachement au réseau des dispositifs et des passerelles MOC;
 - d) surveiller la connectivité de réseau des dispositifs et des passerelles MOC.

9.1.7 Différenciation et traitement des données

Compte tenu des exigences définies dans la section 8.17 concernant la différenciation et le traitement des données collectées, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 1) Il est recommandé qu'un réseau NGN soit capable d'identifier les données en fonction des catégories applicables.
- 2) Il est recommandé qu'un réseau NGN applique différents traitements de données (par exemple, mise en cache et/ou transmission) en fonction de l'identification des données.

9.1.8 Collaboration d'applications et environnement d'intégration et de fourniture de services

Compte tenu des exigences de service définies dans les sections 8.5 et 8.6, les réseaux NGN sont soumis aux exigences supplémentaires suivantes:

- 1) Il est exigé qu'un réseau NGN fournisse des capacités pour la collaboration d'applications et pour un environnement d'intégration et de fourniture de services.

NOTE – Les capacités définies dans [UIT-T Y.2240] peuvent être utilisées pour prendre en charge les exigences précédentes.

9.2 Exigences prises en charge par les capacités NGN existantes

Compte tenu des exigences de service définies dans la section 8, la présente section décrit les exigences prises en charge par les capacités NGN existantes pour la prise en charge des applications MOC.

9.2.1 Gestion par groupe

Les exigences relatives à la gestion par groupe définies dans la section 8.12 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201].

9.2.2 Gestion de la localisation

Un réseau NGN fournit des capacités de gestion de la localisation, qui permettent de déterminer les informations de localisation des utilisateurs et des dispositifs dans le réseau NGN et de transmettre ces informations. Les exigences relatives à la gestion de la localisation définies dans la section 8.11 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201].

9.2.3 Sécurité

Un réseau NGN fournit des capacités de sécurité. Les exigences de services définies dans la section 8.13 sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201] et [UIT-T Y.2701].

9.2.4 Modes de communication liés aux groupes

Compte tenu des exigences de service définies dans la section 8.12, il est exigé qu'un réseau NGN prenne en charge les modes de communication suivants pour les groupes MOC (avec des dispositifs et des passerelles MOC connectés directement ou indirectement aux réseaux NGN):

- unidiffusion;
- multidiffusion;
- radiodiffusion.

Ces exigences sont prises en charge par les capacités existantes des réseaux NGN définies dans [UIT-T Y.2201].

10 Exigences de capacité d'un domaine de dispositifs MOC

La présente section définit les exigences de capacité d'un domaine de dispositifs MOC pour la prise en charge des applications MOC.

10.1 Mise à disposition de capacités pour les applications

Compte tenu des exigences définies dans la section 8.4, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est recommandé que les dispositifs MOC prennent en charge un ensemble d'opérations abstraites.
- 2) Il est recommandé que les dispositifs MOC prennent en charge la mise en oeuvre d'une logique de service pour fournir des capacités MOC.
- 3) Les passerelles MOC peuvent, à titre d'option, prendre en charge un ensemble d'opérations abstraites sur les dispositifs MOC.
- 4) Les passerelles MOC peuvent, à titre d'option, prendre en charge la mise en oeuvre d'une logique de service pour fournir des capacités MOC.

10.2 Mobilité

Compte tenu des exigences définies dans la section 8.1, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les dispositifs et les passerelles MOC prennent en charge des capacités de gestion de mobilité améliorée, afin de prendre en charge différents niveaux de mobilité.

10.3 Communication

Compte tenu des exigences définies dans les sections 8.2, 8.3 et 8.4, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les passerelles et les dispositifs MOC soient capables de créer, de maintenir ou de libérer des ressources de communication, en fonction des besoins des communications de données.
- 2) Il est exigé que les passerelles MOC soient capables de sélectionner les trajets de routage appropriés entre l'extrémité d'émission du trafic (dispositifs MOC ou serveur d'application MOC) et l'extrémité de réception du trafic (dispositifs MOC ou serveur d'application MOC), compte tenu de l'application à laquelle est associé le dispositif, ou inversement.
- 3) Il est exigé que les passerelles MOC permettent de définir et de modifier les horaires et la durée des intervalles de temps pendant lesquels l'accès aux communications de réseau est autorisé ou interdit.

- 4) Il est exigé que les passerelles MOC prennent en charge les modes de communication suivants, en fonction des exigences de service:
 - unidiffusion
 - multidiffusion
 - radiodiffusion.
- 5) Il est recommandé que les passerelles MOC prennent en charge les communications avec des dispositifs propriétaires (par exemple, des dispositifs munis d'interfaces propriétaires pour interfonctionner avec des entités de réseau).
- 6) Il est exigé que les dispositifs MOC passent en mode hors ligne lorsqu'aucune transmission de données n'est requise, puis entrent ensuite en mode veille conformément aux politiques nécessaires.
NOTE – Le passage en mode veille peut aussi être commandé par le réseau.
- 7) Les dispositifs MOC peuvent, à titre d'option, prendre en charge les communications avec le réseau, conformément aux critères suivants: charge de trafic quotidienne sur le réseau, localisation des dispositifs MOC, horaires et durée des intervalles de temps d'accès.

10.4 Qualité de service

Compte tenu des exigences définies dans les sections 8.2 et 8.13, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les passerelles et les dispositifs MOC prennent en charge la politique de commande du trafic qui définit les horaires et la durée des intervalles de temps pendant lesquels l'accès aux communications de réseau est autorisé.
- 2) Il est exigé que les passerelles et les dispositifs MOC prennent en charge la différenciation de la qualité de service, en fonction des différentes catégories de trafic.
- 3) Il est exigé que les passerelles et les dispositifs MOC assurent la mesure et la gestion des performances.
- 4) Il est recommandé que les passerelles et les dispositifs MOC prennent en charge la hiérarchisation des applications.

10.5 Gestion à distance

Compte tenu des exigences définies dans la section 8.9.1, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les passerelles MOC jouent le rôle de mandataire de gestion pour les dispositifs MOC du réseau MOC local connecté. Cette tâche comprend la prise en charge des demandes de gestion provenant du réseau NGN et la gestion locale (vis-à-vis du réseau local MOC) des micrologiciels et des logiciels.
- 2) Il est exigé que les dispositifs MOC prennent en charge la gestion des logiciels et des micrologiciels.
- 3) Il est exigé que les passerelles et les dispositifs MOC prennent en charge la gestion de la configuration.
- 4) Il est exigé que les passerelles MOC prennent en charge la collecte et le stockage des données concernant les dérangements et la performance.
- 5) Il est recommandé que les dispositifs MOC prennent en charge la collecte et le stockage des données concernant les dérangements et la performance.

10.6 Adressage et identification des dispositifs

Compte tenu des exigences définies dans les sections 8.10 et 8.12, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les passerelles MOC prennent en charge l'établissement d'une correspondance entre l'identification d'un dispositif MOC et une ou plusieurs adresses de réseau MOC local.
- 2) Il est exigé que les passerelles MOC prennent en charge l'établissement d'une correspondance entre l'identification d'un groupe de dispositifs MOC et une ou plusieurs adresses de réseau MOC local pour chacun des dispositifs MOC au sein du groupe.
- 3) Il est exigé que les dispositifs MOC prennent en charge une identification unique dans le contexte d'une application MOC unique.
- 4) Une passerelle MOC peut, à titre d'option, utiliser des identifiants temporaires pour les dispositifs MOC qui se connectent au réseau et se déconnectent du réseau de manière dynamique.
- 5) Une passerelle MOC peut, à titre d'option, réassigner des identifiants temporaires libérés de manière dynamique à d'autres dispositifs MOC.

10.7 Sécurité

Compte tenu des exigences définies dans la section 8.14, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est exigé que les passerelles MOC identifient et authentifient les applications MOC, les autres dispositifs MOC et les utilisateurs finals MOC.
- 2) Il est exigé que les passerelles MOC prennent en charge des mécanismes de sécurisation du transport, tels que le cryptage et la protection de l'intégrité.
- 3) Il est recommandé que les dispositifs MOC identifient et authentifient les applications MOC, les autres dispositifs MOC et les utilisateurs finals MOC.
- 4) Il est recommandé que les dispositifs MOC prennent en charge des mécanismes de sécurisation du transport, tels que le cryptage et la protection de l'intégrité.

10.8 Comptabilité et taxation

Compte tenu des exigences définies dans la section 8.8, les exigences suivantes s'appliquent aux capacités des passerelles et des dispositifs MOC:

- 1) Il est recommandé que les passerelles MOC prennent en charge différentes méthodes de comptabilité et de taxation pour les dispositifs MOC connectés.

10.9 Identification des données

Compte tenu des exigences relatives à la différenciation des données collectées et au traitement associé de ces données définies dans la section 8.17, les exigences suivantes s'appliquent aux capacités des dispositifs et des passerelles MOC:

- 1) Il est recommandé que les passerelles MOC rendent les données identifiables conformément aux politiques applicables.
- 2) Les dispositifs MOC peuvent, à titre d'option, rendre les données identifiables conformément aux politiques applicables.

11 Cadre de référence pour les capacités MOC

11.1 Vue de haut niveau

La Figure 11-1 présente une vue de haut niveau du cadre de référence pour les capacités MOC.

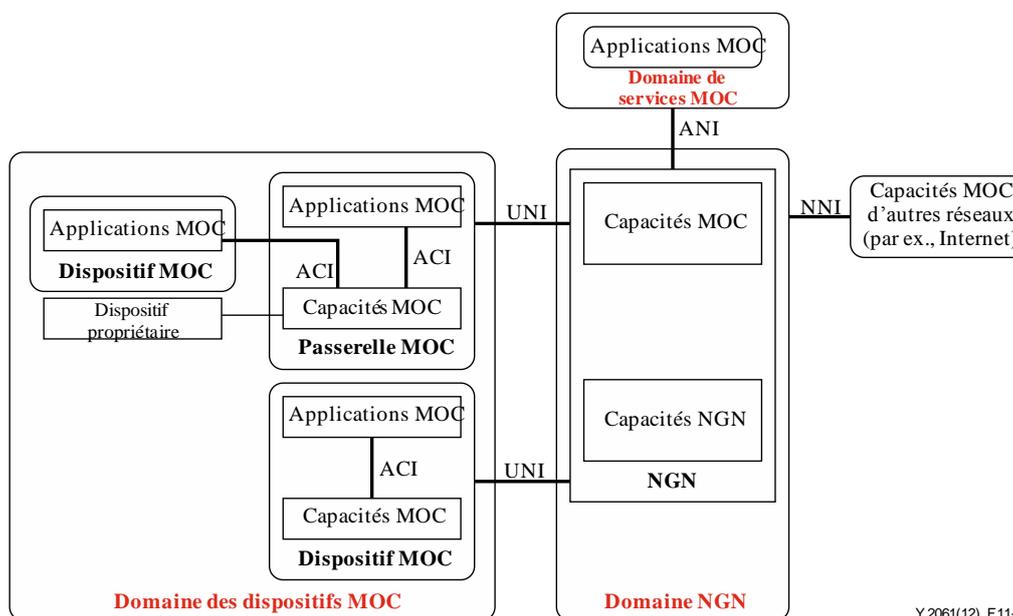


Figure 11-1 – Vue de haut niveau du cadre de référence pour les capacités MOC

Le domaine de dispositifs MOC comprend des dispositifs MOC, des dispositifs propriétaires et des passerelles MOC. Les capacités MOC du domaine de dispositifs MOC collaborent avec les capacités MOC et les capacités NGN du domaine NGN afin de prendre en charge les applications MOC.

L'interface entre les dispositifs ou les passerelles MOC et le réseau NGN est l'interface utilisateur-réseau (UNI).

L'interface entre les capacités MOC et les applications MOC résidant dans le domaine de dispositifs MOC est l'interface application-capacités (ACI).

Le domaine NGN comprend:

- des capacités NGN (modifiées et étendues, si nécessaire, pour la prise en charge des applications MOC, comme indiqué dans la section 9);
- des capacités MOC.

L'interface entre le réseau NGN et les autres réseaux est l'interface réseau-réseau (NNI).

Le domaine de services MOC comprend des applications MOC.

L'interface entre le réseau NGN et les applications MOC résidant dans le domaine de services MOC est l'interface application-réseau (ANI).

Afin de prendre en charge les applications MOC, des interfaces de service sont fournies à travers les interfaces ACI, ANI, NNI et UNI. Les exigences de ces interfaces de service sont définies dans la section 11.4.

11.2 Capacités MOC dans le domaine NGN

Les principales capacités MOC dans le domaine NGN sont décrites dans la Figure 11-2. Ces capacités fournissent des interfaces normalisées pour les applications MOC aux dispositifs et aux passerelles MOC, aux fins de la collecte, de la gestion et de l'exploitation des données.

Les capacités MOC présentées dans la Figure 11-2 sont définies dans [UIT-T Y.2240] et adaptées, si nécessaire, au contexte des communications MOC.

Comme indiqué dans [UIT-T Y.2240], les capacités MOC interagissent aussi avec les capacités NGN définies dans [UIT-T Y.2201], avec des capacités IT ou avec des capacités Internet.

NOTE 1 – Les capacités NGN dans le domaine NGN se situent à l'intérieur de la strate des services NGN définie dans [UIT-T Y.2012].

NOTE 2 – Il n'est pas exclu que d'autres capacités définies dans [UIT-T Y.2240] fassent partie des capacités MOC dans le domaine NGN, moyennant au besoin une adaptation, comme indiqué dans la Figure 11-2.

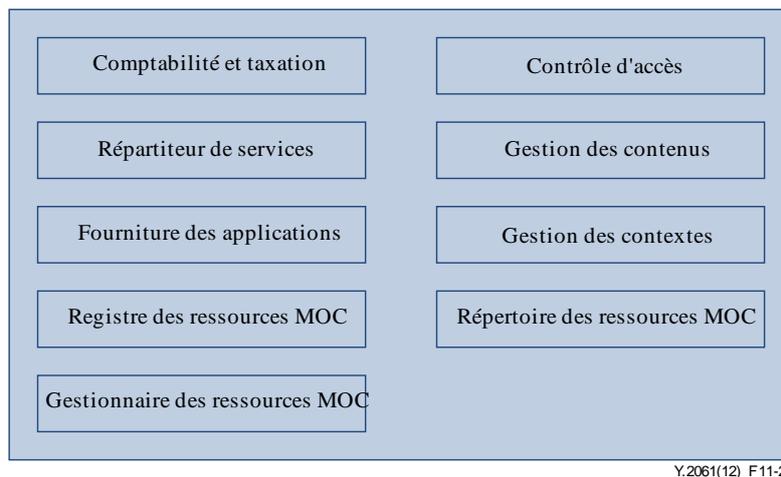


Figure 11-2 – Capacités MOC dans le domaine NGN

11.2.1 Comptabilité et taxation

Cette capacité prend en charge des modes et des mécanismes de comptabilité et de taxation pour les applications MOC, y compris :

- la prise en charge du partage des recettes entre les différents acteurs de l'écosystème MOC;
- la prise en charge de la taxation en ligne et hors ligne basée sur les événements dans l'écosystème MOC.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.2 Contrôle d'accès

Cette capacité assure l'authentification et l'autorisation des applications MOC avant de les autoriser à accéder à un ensemble de capacités spécifiques. La capacité de contrôle d'accès assure la traduction des interfaces de programmation d'application (API) et des protocoles dans différentes interfaces de service, ainsi que l'accès, à partir des applications, aux fonctionnalités exposées par les capacités MOC.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.3 Répartiteur de services

Cette capacité fournit des mécanismes unifiés pour l'acheminement et l'échange de messages entre les capacités MOC dans le domaine NGN.

Le répartiteur de services assure également la transformation des interfaces API et des protocoles depuis les applications MOC vers des types courants de structure de message et de traitement des événements opérationnels, et inversement.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.4 Gestion des contenus

Les contenus peuvent être fournis à titre de ressources à une application ou à des utilisateurs finals MOC par différents fournisseurs de dispositifs MOC (par exemple, fournisseurs de contenus et utilisateurs finals).

La capacité de gestion des contenus assure l'extraction des informations pertinentes (y compris la taille, le type et la localisation) à partir des contenus, afin que les capacités MOC dans le domaine NGN puissent garantir l'intégrité des contenus eux-mêmes.

La capacité de gestion des contenus établit au besoin le profil des contenus, en vue de leur fourniture à différentes applications MOC; par exemple, des contenus peuvent être destinés à des applications MOC particulières ou à un utilisateur final MOC particulier.

La capacité de gestion des contenus assure la répartition des contenus en vue de leur exposition aux applications.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.5 Fourniture des applications

Cette capacité sert à assurer le déploiement sécurisé des applications par le fournisseur d'applications MOC, lorsque les applications sont prêtes à être déployées. Cette capacité assure le conditionnement, la publication, le déploiement, la gestion du cycle de vie et les fonctions de surveillance des applications.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.6 Gestion des contextes

Cette capacité collecte, agrège et gère les informations de contexte relatives aux différentes sources de contexte. Elle expose les informations de contexte, notamment à d'autres capacités MOC, conformément aux politiques du fournisseur d'applications MOC.

Pour de plus amples informations concernant cette capacité, voir [UIT-T Y.2240].

11.2.7 Registre des ressources MOC

Cette capacité fournit les fonctionnalités relatives à l'enregistrement, au désenregistrement, à la découverte et à la gouvernance des ressources mises à disposition par les fournisseurs de dispositifs MOC. Des descriptions des ressources orientées vers l'enregistrement, y compris l'identification et l'adressage uniques des ressources, sont publiées dans le registre des ressources MOC.

Cette capacité définit un mécanisme servant à enregistrer une ressource d'un fournisseur de dispositifs MOC dans les capacités MOC du domaine NGN, afin que les applications puissent localiser cette ressource et y avoir accès.

Du point de vue fonctionnel, cette capacité correspond à la capacité de registre des ressources définie dans [UIT-T Y.2240], adaptée au contexte des communications MOC.

11.2.8 Répertoire des ressources MOC

Cette capacité fournit des fonctionnalités pour le stockage des informations relatives aux ressources MOC enregistrées. Stockées dans le répertoire des ressources MOC, les informations relatives aux ressources MOC sont accessibles aux applications MOC authentifiées et autorisées. Les informations relatives aux ressources enregistrées comprennent différents outils de conditionnement appropriés à l'intention des développeurs d'applications.

Du point de vue fonctionnel, cette capacité correspond à la capacité de répertoire des ressources définie dans [UIT-T Y.2240], adaptée au contexte des communications MOC.

11.2.9 Gestionnaire des ressources MOC

Cette capacité assure les fonctions de contrôle des ressources fournies par le réseau NGN et les dispositifs MOC afin de répondre aux besoins des applications MOC, y compris la gestion des informations dynamiques concernant l'état de disponibilité des dispositifs MOC (par exemple, en ligne/hors ligne, transmission de données en cours).

Du point de vue fonctionnel, cette capacité correspond à la capacité de gestionnaire des ressources définie dans [UIT-T Y.2240], adaptée au contexte des communications MOC.

11.3 Capacités MOC dans le domaine de dispositifs MOC

Les capacités MOC dans le domaine MOC sont présentées dans la Figure 11-3.

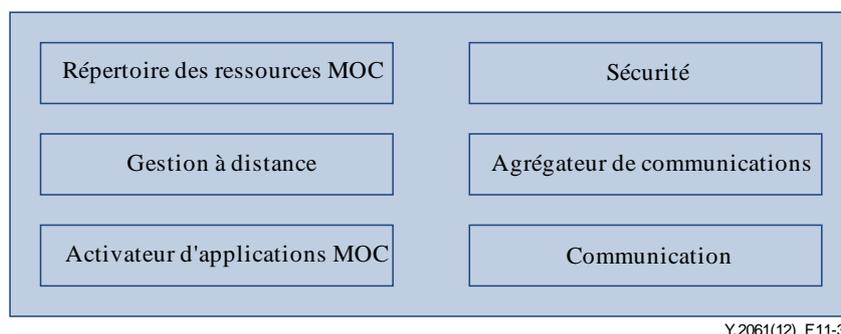


Figure 11-3 – Capacités MOC dans le domaine de dispositifs MOC

11.3.1 Agrégateur de communications

Cette capacité, qui réside dans les passerelles MOC, assure des fonctions de procuration et d'agrégation de trafic.

Compte tenu des exigences définies dans la section 10.3, la capacité d'agrégateur de communications prend en charge le relai du trafic entre les dispositifs MOC et les réseaux NGN, des mécanismes de qualité de service basés sur la politique d'applications MOC et l'enregistrement des informations de taxation pour les dispositifs MOC du réseau MOC local.

11.3.2 Mise à disposition de capacités pour les applications MOC

Compte tenu des exigences définies dans la section 10.1, cette capacité expose aux applications MOC les capacités MOC résidant dans les passerelles et les dispositifs MOC.

11.3.3 Répertoire des ressources MOC

Compte tenu des exigences définies dans la section 10.1, cette capacité, qui réside dans les passerelles MOC, fournit des fonctionnalités pour le stockage des informations relatives aux dispositifs MOC enregistrés. Stockées dans le répertoire des dispositifs MOC, les données des dispositifs MOC peuvent être lues par les applications MOC authentifiées et autorisées.

11.3.4 Gestion à distance

Compte tenu des exigences définies dans la section 10.5, cette capacité prend en charge la gestion de la configuration, la gestion des dérangements, la gestion de la performance et la mise à niveau des logiciels et des micrologiciels des passerelles et des dispositifs MOC dans le réseau MOC local.

NOTE – Les fonctions précédentes peuvent aussi être réalisées par des capacités de gestion locale des dispositifs et des passerelles MOC.

11.3.5 Sécurité

Compte tenu des exigences définies dans la section 10.7, cette capacité assure l'enregistrement et l'authentification mutuelle avec les applications MOC.

La capacité de sécurité assure le cryptage et la protection de l'intégrité sur les données échangées avec le réseau NGN et les applications MOC, afin de garantir une fourniture sécurisée.

La capacité de sécurité assure la gestion des clés sur la base des clés de service générées dans les dispositifs MOC, et la protection contre l'accès d'applications non autorisées aux dispositifs MOC.

11.3.6 Communication

Compte tenu des exigences définies dans les sections 10.3, 10.6, 10.8 et 10.9, cette capacité assure les fonctions de communication générique dans les dispositifs et les passerelles MOC.

La capacité de communication assure des fonctions de transport des données d'application; fournit des données aux applications MOC et reçoit des données en provenance de ces applications, conformément aux critères de service (par exemple, charge de trafic quotidienne sur le réseau, localisation des dispositifs MOC, horaires et durée des intervalles de temps d'accès); et traite ces données.

11.4 Interfaces de service MOC

Les interfaces de service MOC prennent en charge:

- les applications MOC hébergées dans des dispositifs et des passerelles MOC qui accèdent aux réseaux NGN par l'interface UNI;
- les applications MOC hébergées dans des dispositifs et des passerelles MOC qui accèdent aux capacités MOC hébergées dans la passerelle MOC par l'interface ACI;
- les applications MOC hébergées dans des dispositifs MOC qui accèdent aux capacités MOC hébergées dans ces mêmes dispositifs MOC par l'interface ACI;
- les applications MOC hébergées dans le domaine de services MOC qui accèdent au réseau NGN par l'interface ANI;
- les applications MOC hébergées dans le domaine de services MOC, qui accèdent aux capacités MOC d'autres réseaux par l'interface NNI.

Les applications MOC hébergées dans des dispositifs et des passerelles MOC peuvent être invoquées par un utilisateur final MOC et par d'autres applications MOC, par exemple des applications MOC hébergées dans le domaine de services MOC.

Il est recommandé que les interfaces de service MOC mettent en oeuvre des interfaces API, des protocoles et des technologies normalisés pour réaliser l'exposition des services à destination des applications MOC.

11.4.1 Exigences de l'interface de service à travers l'ACI

L'interface de service à travers l'ACI sert à assurer l'interaction dans le domaine de dispositifs MOC entre les capacités MOC des dispositifs et des passerelles et les applications MOC des dispositifs et des passerelles. L'interface de service à travers l'ACI permet à une application qui réside dans un dispositif MOC d'accéder à des capacités MOC dans le même dispositif MOC ou dans une passerelle MOC. Elle permet aussi à une application résidant dans une passerelle MOC d'accéder à des capacités MOC dans la même passerelle MOC.

Il est exigé que l'interface ACI permette de réaliser les fonctions suivantes:

- enregistrement des dispositifs et des passerelles MOC auprès des capacités résidant dans le dispositif et la passerelle MOC (par exemple, enregistrement d'un capteur ou d'un GPS à bord d'une voiture auprès de la passerelle qui se trouve dans la voiture);
- demandes émises par des applications MOC visant à l'exécution de tâches spécifiques à un dispositif MOC par un dispositif et une passerelle MOC ou par un groupe de dispositifs et de passerelles MOC;
- abonnement à des événements particuliers et notification associée (par exemple, abonnement mutuel à des événements particuliers et notification associée (par exemple, connectivité des dispositifs et des passerelles MOC) entre des capacités et des applications MOC);
- demandes des dispositifs et des passerelles MOC visant à la création ou à la suppression de groupes ou concernant la liste des membres de groupes.

11.4.2 Exigences de l'interface de service à travers l'UNI

L'interface de service à travers l'UNI sert à assurer l'interaction entre les capacités MOC des dispositifs et des passerelles MOC et les capacités MOC du réseau NGN. Il est recommandé que l'interface UNI prenne en charge des interfaces API normalisées pour exposer les ressources fournies par le domaine de dispositifs MOC aux capacités MOC dans le domaine NGN.

Il est exigé que l'interface UNI permette de réaliser les fonctions suivantes:

- enregistrement des capacités MOC dans le domaine de dispositifs MOC auprès des capacités MOC dans le domaine NGN;
- demande émise par des dispositifs MOC visant à l'exécution d'une tâche spécifique devant être effectuée par une application MOC;
- abonnement à des événements particuliers et notification associée émanant du domaine de dispositifs MOC ou à destination du domaine de dispositifs MOC;
- demandes visant à créer ou à supprimer des groupes ou concernant la liste des membres de groupes.

11.4.3 Exigences de l'interface de service à travers l'ANI

Les demandes de services émises par les applications MOC sont envoyées aux capacités MOC dans le domaine NGN par l'intermédiaire de l'interface ANI. Il est exigé que l'interface de service à travers l'ANI assure l'interaction entre les applications MOC dans le domaine de services MOC et les capacités MOC dans le domaine NGN.

Il est recommandé que l'interface ANI prenne en charge des interfaces API normalisées pour exposer les ressources fournies par le domaine NGN aux applications MOC.

Il est exigé que l'interface ANI permette de réaliser les fonctions suivantes:

- enregistrement des applications MOC auprès des capacités MOC dans le domaine NGN;
- demande émise par des applications MOC visant à l'exécution d'une tâche spécifique devant être effectuée par un dispositif et une passerelle MOC ou par un groupe de dispositifs et de passerelles MOC;
- abonnement à des événements particuliers et notification associée émanant d'applications MOC ou à destination d'applications MOC;
- demandes visant à créer ou à supprimer des groupes ou concernant la liste des membres de groupes.

11.4.4 Exigences de l'interface de service à travers la NNI

L'interface de service à travers la NNI sert à assurer l'interaction avec les capacités MOC d'autres réseaux. L'interface de service suivante à travers la NNI est pertinente du point de vue de l'interaction des réseaux NGN avec les capacités MOC d'autres réseaux:

- interface de service entre des réseaux NGN et d'autres réseaux (NGN ou non NGN), chacun des deux réseaux étant doté de capacités pour la prise en charge des applications MOC.

NOTE – Le cas d'une interaction NNI entre un réseau NGN et d'autres réseaux dépourvus de capacités pour la prise en charge des applications MOC n'est pas pertinent, étant donné qu'il suppose uniquement une interaction au niveau transport.

12 Considérations relatives à la sécurité

Les exigences de sécurité pour les applications MOC sont décrites dans la section 8.14.

Les exigences de sécurité pour le domaine NGN sont définies dans la section 9.2.5.

Les exigences de sécurité pour le domaine de dispositifs MOC sont définies dans la section 10.7.

Appendice I

Acteurs et rôles associés dans l'écosystème MOC

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

Les points suivants définissent différents acteurs de l'écosystème MOC et les rôles opérationnels (voir la section 6.3) qu'ils peuvent jouer:

- **Le "transporteur"**. Le "transporteur" joue le rôle de fournisseur de réseau. Selon le scénario opérationnel, le "transporteur" peut aussi jouer le rôle de fournisseur d'applications MOC, de fournisseur de plates-formes MOC et de fournisseur de dispositifs MOC.
- **Le "fournisseur d'applications tierces"**. Le "fournisseur d'applications tierces" joue le rôle de fournisseur d'applications MOC. Les fournisseurs d'applications web sont un exemple de fournisseurs d'applications tierces. Le "fournisseur d'applications tierces" peut aussi jouer (sans toutefois s'y limiter) le rôle de fournisseur de plates-formes MOC.
- **Le "fournisseur de dispositifs tiers"**. Le "fournisseur de dispositifs tiers" joue le rôle de fournisseur de dispositifs MOC. Les opérateurs de dispositifs MOC et les utilisateurs finals sont des exemples de fournisseurs de dispositifs tiers. Le "fournisseur de dispositifs tiers" peut aussi jouer (sans toutefois s'y limiter) le rôle de fournisseur de plates-formes MOC, de fournisseur d'applications MOC et de client d'applications MOC.

Appendice II

Cas d'utilisation des communications MOC

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

II.1 Cybersanté

La cybersanté est un terme relativement récent qui désigne les pratiques de soins de santé reposant sur l'utilisation de processus et de communications électroniques.

Le Figure II.1 présente un exemple de configuration de service de cybersanté.

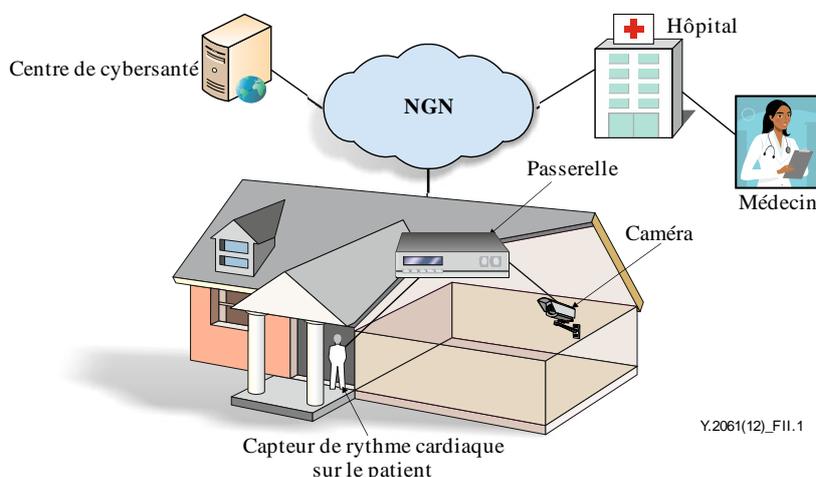


Figure II.1 – Configuration d'un service de cybersanté

Différents types de dispositifs sont utilisés pour fournir des services de cybersanté. Certains de ces dispositifs ne font que collecter des données et interagir avec le réseau (par exemple, les capteurs de rythme cardiaque), alors que d'autres peuvent interagir de manière bidirectionnelle (par exemple, les caméras). Certains dispositifs produisent généralement de faibles quantités de données (par exemple, les thermomètres), alors que d'autres génèrent des flux multimédias (par exemple, les caméras) ou assurent une fonction de commande de session d'appel (par exemple, les terminaux SIP qui prennent en charge les appels vidéo). Certains dispositifs peuvent même assurer à la fois les fonctions de plateformes de passerelles et de plates-formes de services de type capteur.

Les dispositifs de cybersanté collectent des données et les envoient aux parties concernées, telles que le centre de cybersanté dans la Figure II.1. Les hôpitaux, les médecins et les familles peuvent s'abonner au service pour obtenir des données brutes ou traitées.

Les dispositifs liés aux patients peuvent accéder au réseau directement ou par l'intermédiaire d'une ou de plusieurs passerelles (par exemple, passerelle domestique ou passerelle portée sur soi):

- 1) Lorsque les patients restent à l'intérieur, les dispositifs peuvent accéder au réseau à l'aide d'une passerelle domestique statique unique ou de plusieurs passerelles domestiques dynamiques (dans le second cas, les patients peuvent se déplacer et accéder au réseau à l'aide de différentes passerelles).
- 2) Lorsque les patients sont à l'extérieur, les dispositifs peuvent accéder au réseau directement à l'aide d'un réseau mobile, ou indirectement à l'aide d'une passerelle portée sur soi.

Les problèmes techniques suivants doivent être pris en compte dans le contexte de la cybersanté:

- Les groupements devraient être pris en charge. Cette fonction est utile, par exemple, dans le cas où plusieurs patients ont le même type de maladie, ou encore dans le cas d'un seul patient, pour gérer un ensemble de dispositifs qui peuvent faire l'objet d'une gestion par groupe.

- La commande optimisée du trafic devrait être prise en charge. Par exemple, il se peut que les données détectées soient de très petite taille et qu'il soit nécessaire de les transmettre au réseau toutes les heures: dans ce cas, le fait d'être connecté au réseau en permanence représente un gaspillage de ressources. Le réseau devrait être optimisé en termes de commande du trafic, et, en pareil cas, le trafic pourrait être acheminé, par exemple, à l'aide d'une signalisation de plan d'utilisateur sans support IP dédié aux données. De plus, des dispositifs portés par un patient pourraient rester en mode veille et se réveiller lorsque le médecin doit faire un diagnostic à distance au patient.
- Différents niveaux de mobilité devraient être pris en charge. Par exemple, dans le cas de patients à mobilité limitée (qui se déplacent peu fréquemment et sur de courtes distances), le fait d'activer la totalité des capacités de gestion de la mobilité représente un gaspillage de ressources.
- L'activation et la gestion à distance des dispositifs devraient être prises en charge. Par exemple, les dispositifs en mode veille ne devraient être réveillés que lorsque le médecin doit faire un diagnostic à distance au patient.
- La temporisation devrait être prise en charge. Par exemple, il peut arriver que les dispositifs portés par les patients collectent de nombreuses données, mais qu'ils n'aient pas toujours à les transmettre à chaque collecte, compte tenu du caractère non essentiel de ces données (par exemple, données concernant seulement un examen de routine). En pareil cas, le réseau peut affecter des intervalles de temps spécifiques à la transmission des données des dispositifs (en dehors de ces intervalles, les dispositifs ne peuvent pas transmettre de données ou sont soumis à des taux de taxation plus élevés).
- Les profils de dispositifs devraient être pris en charge. Les patients peuvent acheter de nouveaux dispositifs et les connecter au réseau de manière dynamique: les informations relatives aux dispositifs devraient être intégrées dans les profils de dispositif et mises à jour de manière dynamique, afin que les dispositifs nouvellement ajoutés puissent être authentifiés et commandés par le réseau, et aussi être supprimés.
- Les dispositifs placés derrière une passerelle devraient pouvoir être identifiés par le réseau. La passerelle pourrait fournir uniquement un canal support et jouer le rôle d'agrégateur de données pour les dispositifs qui lui sont connectés, ou fournir une commande de service à ces dispositifs. Dans le premier cas, les dispositifs connectés à la passerelle devraient être commandés par le réseau, ou à la fois par le réseau et par la passerelle.
- Les dispositifs propriétaires devraient être pris en charge. Un grand nombre de dispositifs et de passerelles propriétaires sont exploités sur les réseaux: l'adaptation aux dispositifs et aux passerelles propriétaires existants devrait être prise en charge.
- Les profils de service devraient être pris en charge. En général, les patients ne connaissent pas très bien les services offerts par différents hôpitaux, et peuvent seulement se connecter au portail du centre de cybersanté et accéder aux services. Le centre de cybersanté, en revanche, connaît généralement bien ces services et peut déterminer les hôpitaux les plus indiqués compte tenu de leurs connaissances professionnelles. Un ou plusieurs hôpitaux peuvent fournir conjointement des services médicaux à un patient. En d'autres termes, lorsque les dispositifs placés sur un patient transmettent des données au centre de cybersanté, celui-ci peut habilement aider le patient à choisir les hôpitaux les plus indiqués et communiquer les données à ces hôpitaux en vue de l'établissement d'un diagnostic commun. Dans ce cas de figure, des sessions de commande d'appel multimédia (audio, vidéo, messagerie de texte, etc.) pourraient être nécessaires. En outre, les dispositifs devraient interagir avec plusieurs applications.

Lorsque des médecins font des diagnostics et fournissent des services de soins de santé à distance, ils ont en général aussi besoin du système de diagnostic ou du système de base de données internes existants de l'hôpital pour les aider: les données transmises par les dispositifs peuvent alimenter le

système interne existant de l'hôpital. Dans ce cas, les dispositifs devraient être interopérables avec les systèmes existants (par exemple, format des données, invocation des capacités de service, etc.), c'est-à-dire que le système de cybersanté devrait être capable de collaborer et d'interfonctionner avec les systèmes d'application existants, qui sont généralement hétérogènes.

- L'équilibrage de la charge de trafic devrait être pris en compte en vue de faire face à des situations particulières. Par exemple, en raison de la très grande variabilité du nombre de patients entre différentes zones, le taux de patients peut être relativement élevé dans les départements de gériatrie, dans les communautés de personnes âgées et dans certaines villes, en comparaison d'autres villes. Le réseau devrait être capable de gérer en conséquence le déséquilibre du système dans des situations particulières qui occasionnent un trafic ou une charge de service élevés, notamment dans le cas des services de type vidéo (par exemple, lorsque de nombreux patients utilisent le diagnostic à distance par vidéo).

II.2 Service d'alerte aux tsunamis

Le système d'alerte aux tsunamis sert à détecter les tsunamis et à émettre des alertes afin d'éviter les pertes de vies humaines et de biens.

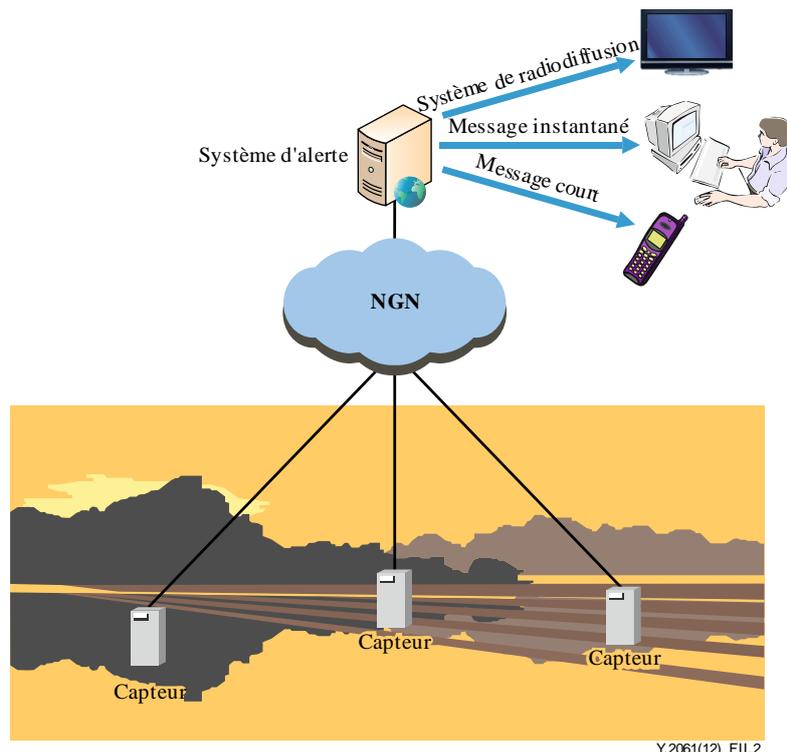


Figure II.2 – Configuration du service d'alerte aux tsunamis

Comme le montre la Figure II.2, il comprend deux parties aussi importantes l'une que l'autre: un réseau de capteurs pour détecter les tsunamis et une infrastructure de communication pour émettre des alertes rapides destinées à faciliter l'évacuation des zones côtières. La détection et la prévision des tsunamis ne représentent que la moitié de la tâche du système. L'autre partie, tout aussi importante, est la capacité à avertir les habitants des zones qui seront touchées. Pour augmenter les chances de sauver des vies, il convient d'élaborer des consignes d'évacuation adaptées à la situation des personnes en danger (par exemple, heure, lieu et contexte). Si un visiteur se rend de nuit dans une zone qu'il ne connaît pas, une simple alarme est insuffisante pour lui permettre de fuir vers un lieu sûr. Tous les systèmes d'alerte aux tsunamis comportent plusieurs lignes de communications (par exemple, SMS, courriel, fax, radio, texte et télex, qui utilisent souvent des systèmes dédiés renforcés), qui permettent l'envoi de messages d'urgence aux services d'urgence et aux forces armées, ainsi qu'aux systèmes

d'alerte à la population (par exemple, sirènes). Dans ce cas d'utilisation, il est exigé que le service prenne en charge:

- l'interfonctionnement avec des réseaux hétérogènes, y compris les réseaux des médias de masse (par exemple, radio, télévision) et les systèmes de communication dédiés (par exemple, sirènes);
- la fourniture d'informations d'urgence, qui comprennent à la fois les informations primaires produites par le détecteur et les informations secondaires transmises à la population cible;
- la fourniture d'informations d'urgence sur de multiples réseaux, au moyen de supports fiables et non fiables (par exemple, communications à l'aide de systèmes par satellite), de manière à optimiser la probabilité de transmission des informations;

NOTE – La question de l'intégrité des informations, qui pourrait être compromise par des supports fiables et non fiables, nécessite des études supplémentaires.

- la robustesse du système, c'est-à-dire que le système devrait pouvoir faire face à la production d'une très grande quantité d'informations sur une courte période en raison de la présence d'un grand nombre de dispositifs (par exemple, détecteurs ou capteurs d'urgence) dans une zone;
- la fourniture prioritaire des informations d'urgence, c'est-à-dire que les messages d'urgence concernant un tremblement de terre devraient avoir priorité sur les autres messages de service.

II.3 Gestion d'une flotte de véhicules

La Figure II-3 présente la configuration de service type de la gestion d'une flotte de véhicules.

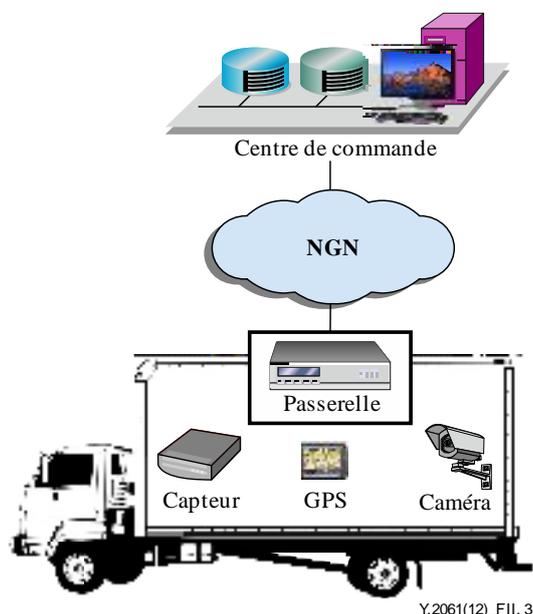


Figure II.3 – Configuration de service type de la gestion d'une flotte de véhicules

Chaque autobus est équipé de dispositifs et de passerelles qui ont les mêmes caractéristiques. Le centre de commande rassemble des données relatives à la localisation, à la vitesse et à la situation relevées par les capteurs, le terminal du Système mondial de positionnement (GPS) et la caméra de l'autobus. Les données agrégées par l'intermédiaire d'une passerelle placée à bord de l'autobus sont transmises au réseau NGN au moyen d'un accès hertzien.

Le centre de commande peut transmettre le tableau dynamique des horaires à l'écran d'affichage de l'arrêt d'autobus, en fonction des informations de localisation qu'il reçoit de l'autobus.

Lorsqu'un capteur placé à bord de l'autobus détecte une situation anormale, comme une odeur d'essence, un signal d'alarme est envoyé au centre de commande.

L'autobus emprunte toujours un itinéraire fixe et ne devrait donc pas s'écarter de routes prédéfinies. Lorsqu'un autobus sort d'une zone donnée, une application devrait être déclenchée. Par exemple, il est possible d'appeler le conducteur de l'autobus ou d'envoyer un message d'alerte au gestionnaire de la flotte au moment où l'autobus quitte la zone.

Dans ce cas d'utilisation, il est exigé que le service prenne en charge:

- le fonctionnement basé sur la localisation: une application devrait être déclenchée lorsque les dispositifs se trouvent à l'intérieur ou à l'extérieur d'une zone donnée;
- la hiérarchisation du niveau de service: par exemple, un message d'alerte devrait avoir priorité sur les autres données;
- la gestion de groupe pour les dispositifs de caractéristiques identiques.

II.4 La maison intelligente

La maison intelligente réunit généralement une combinaison de différents dispositifs et applications, tels que des capteurs en temps réel ou en temps quasi réel, la notification des pannes d'électricité et la surveillance de la qualité énergétique.

La Figure II.4 présente une configuration type de la "maison intelligente".

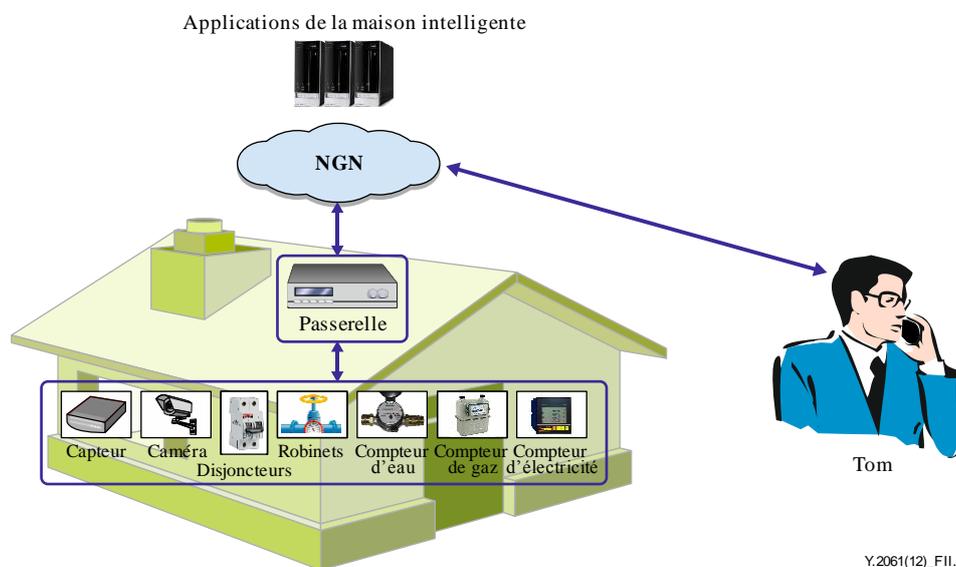


Figure II.4 – Configuration de service type de la maison intelligente

Comme le montre la Figure II.4, la configuration d'une maison intelligente se présente souvent sous la forme de dispositifs (par exemple, détecteurs de fumée, compteurs d'électricité, compteurs de gaz, etc.) connectés à une plate-forme d'applications de la maison intelligente au moyen d'une passerelle qui se trouve dans la maison intelligente. Le centre de données collecte des données par l'intermédiaire des dispositifs de la maison intelligente qu'il peut commander à distance à l'aide de la passerelle. Dans ce cas d'utilisation, les informations concernant la consommation d'électricité, de gaz et d'eau de la maison de Tom peuvent être collectées et transmises à la plate-forme d'applications de la maison intelligente. Dans le même temps, Tom peut gérer la politique de sa maison en matière d'applications à l'aide des applications de la maison intelligente, et la politique relative aux applications peut être envoyée aux dispositifs MOC en vue de son application conformément aux exigences de Tom.

Par exemple, Tom peut définir la politique relative aux applications comme suit:

- 1) Si un détecteur d'incendie détecte des signes d'incendie dans la maison de Tom, alors il envoie un message d'alarme court au téléphone mobile de Tom.

- 2) Si une alarme est déclenchée par un détecteur de bris de porte, alors une communication vidéo est établie afin que Tom puisse voir en temps réel ce qui se passe dans sa maison.

Supposons qu'un voleur fracture une porte de la maison de Tom. Lorsqu'il détecte cet événement, le dispositif MOC (c'est-à-dire le détecteur de bris de porte) établit une communication vidéo entre Tom et une caméra de vidéosurveillance installée dans sa maison. Tom regarde et enregistre la vidéo sur son téléphone mobile (enregistrement qui peut servir de preuve de l'infraction).

Supposons maintenant que Tom est sorti au moment où un incendie se déclare dans sa cuisine, alors que son fils s'y trouve en train de cuisiner. Lorsqu'il détecte cet événement, le dispositif MOC (c'est-à-dire le détecteur d'incendie) envoie directement un message d'alarme à Tom. Lorsqu'il reçoit cette information, Tom établit une communication vidéo avec la caméra pour vérifier l'état de sa cuisine et expliquer à son fils comment utiliser l'extincteur ou sortir. Pour des raisons de confidentialité et de sécurité, seuls des membres de la famille de Tom peuvent se connecter à la caméra et la commander.

Dans ce cas d'utilisation, il est exigé que le service prenne en charge:

- des capacités vidéo/audio évoluées, telles que la diffusion vidéo en continu simultanément avec une sortie de zone locale;
- la gestion par groupe des dispositifs MOC de caractéristiques identiques, par exemple des compteurs d'électricité dans différentes maisons intelligentes;
- la radiodiffusion et la multidiffusion de messages compte tenu de caractéristiques spécifiques, telles que les groupes ou la localisation, afin de prendre en charge des fonctions comme la mise à niveau des micrologiciels.

II.5 Intégration avec les services Internet

De nombreux services attrayants se développent sur l'Internet, tels que les services de réseau social (SNS). Les applications MOC devraient être capables de fonctionner avec ces services Internet, afin de faire en sorte que les clients puissent utiliser les applications MOC avec les services Internet populaires existants. Intégrées avec les services Internet, les applications MOC elles-mêmes étendront leurs chaînes de valeur et attireront davantage de clients.

Dans certains cas d'intégration, les capacités MOC devraient être capables d'appliquer des règles de détection des données (c'est-à-dire d'établir des règles) aux dispositifs et aux passerelles MOC. Une fois détectées, les données devraient être transférées aux capacités MOC dans un format défini. Le formatage des données permet de faciliter les communications entre les capacités MOC et les services Internet qui assurent la publication.

La Figure II.5 présente un exemple de cas d'utilisation de l'intégration d'une application MOC et d'un service Internet.

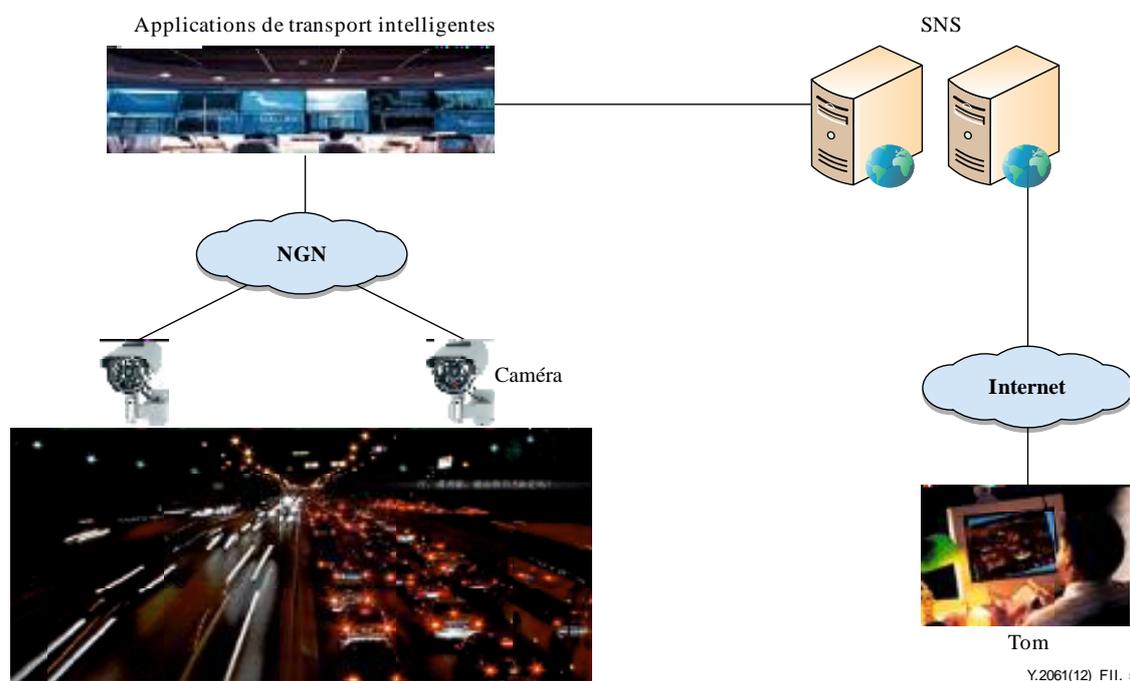


Figure II.5 – Configuration type d'un service Internet

Un fournisseur d'applications MOC propose aux clients un service de transport intelligent. Ce service permet aux clients d'accéder aux contenus qui les intéressent par l'intermédiaire d'un service SNS conformément à leurs règles préférées (par exemple, heures de publication). Le fournisseur collecte les contenus au moyen d'une application MOC et les fournit aux clients au moyen d'un service SNS conformément aux règles définies par les clients.

Tom découvre que le service de transport intelligent fournit des images et des vidéos en temps réel de la circulation de la ville prises par des caméras installées dans les rues, et que ces informations sont fournies au moyen d'un service SNS. Tom s'abonne à ce service (avec, par exemple, mise à jour régulière toutes les cinq minutes) et reçoit en instantané des informations concernant la circulation sur son service SNS.

Le service met à jour les informations par l'intermédiaire du service SNS compte tenu des préférences de Tom. Lorsqu'il rentre chez lui, Tom peut se tenir informé de l'état de la circulation sur les grands axes.

Dans ce cas d'utilisation, il est exigé que le service prenne en charge:

- l'intégration avec les services Internet au moyen des capacités MOC;
- l'établissement de règles pour la détection des données des dispositifs et des passerelles MOC ainsi que pour le transfert de ces données sous un format défini aux capacités utilisées pour communiquer avec les services Internet assurant la publication;
- la possibilité pour les clients d'accéder aux contenus MOC pertinents par l'intermédiaire des services Internet, conformément à des règles définies;
- la détection des contenus MOC pertinents et leur fourniture aux services Internet, conformément aux règles;
- la communication avec les services Internet aux fins de l'échange d'informations.

Bibliographie

- [b-UIT-T Y.2001] Recommandation UIT-T Y.2001 (2004), *Aperçu général des réseaux de prochaine génération.*
- [b-UIT-T Y.2011] Recommandation UIT-T Y.2011 (2004), *Principes généraux et modèle de référence général pour les réseaux de prochaine génération.*
- [b-UIT-T Y.2213] Recommandation UIT-T Y.2213 (2008), *Exigences et capacités liées aux services NGN concernant les aspects réseau des applications et services utilisant une identification par étiquette.*
- [b-UIT-T Y-Sup.7] Recommandations UIT-T de la série Y – Supplément 7 (2008), *Supplément sur le domaine d'application de la version 2 des NGN.*
- [b-UIT-T Q.1741.7] Recommandation UIT-T Q.1741.7 (2011), *Références IMT-2000 à la version 9 du réseau central UMTS issu du GSM.*
- [b-ETSI TS 102 689] ETSI TS 102 689 V1.1.1 (2010), *Machine-to-Machine communications (M2M); M2M service requirements.*
- [b-ETSI TS 102 690] ETSI TS 102 690 V1.1.1 (2011) *Machine-to-Machine communications (M2M); Functional architecture.*
- [b-3GPP TS 22.368] 3GPP TS 22.368 V 11.3.0 (2011), *Service requirements for Machine-Type Communications (MTC).*
- [b-3GPP2-S.R0141-0] 3GPP2 S.R0141-0 V.1.0 (2010), *Study for Machine-to-Machine (M2M) Communication for cdma2000 Networks.*

SÉRIES DES RECOMMANDATIONS UIT-T

Série A	Organisation du travail de l'UIT-T
Série D	Principes généraux de tarification
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	Terminaux et méthodes d'évaluation subjectives et objectives
Série Q	Commutation et signalisation
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 et réseaux de prochaine génération
Série Z	Langages et aspects généraux logiciels des systèmes de télécommunication