Union internationale des télécommunications

UIT-T

SECTEUR DE LA NORMALISATION
DES TÉLÉCOMMUNICATIONS
DE L'UIT

Y.4500.2

(05/2018)

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

Internet des objets et villes et communautés intelligentes – Cadres, architectures et protocoles

oneM2M – Exigences

Recommandation UIT-T Y.4500.2

RECOMMANDATIONS UIT-T DE LA SÉRIE Y

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

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

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

Recommandation UIT-T Y.4500.2

oneM2M – Exigences

Résumé

La Recommandation UIT-T Y.4500.2 présente un modèle informatif des rôles fonctionnels et les exigences techniques normatives pour le système oneM2M.

Historique

Edition	Recommandation	Approbation	Commission d'études	ID unique*
1.0	ITU-T Y.4500.2	2018-05-06	20	11.1002/1000/13499

Mots clés

Communication, exigence, interfonctionnement LWM2M, oneM2M, opérationnel, sécurité, sémantique, système global, tarification.

* 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 2018

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

Recommandation UIT-T Y.4500.2

oneM2M – Exigences

1 Domaine d'application

La présente Recommandation contient un modèle informatif des rôles fonctionnels et les exigences techniques normatives pour le système oneM2M.

La Recommandation contient la version 2 de la spécification oneM2M – Exigences V2.7.1; elle est équivalente aux normes des partenaires de oneM2M, à savoir: ARIB, ATIS [b-ATIS.oneM2M.TS0002V2.7.1], CCSA, ETSI [b-ETSI TS 118 102], TIA, TSDSI, TTA [b-TTA.oneM2M.TS0002V2.7.1] et TTC [b-TTC.oneM2M.TS0002V2.7.1].

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 Y.4500.11] Recommandation UIT-T Y.4500.11 (2018), *oneM2M –Terminologie commune*.

[ETSI TS 122 368] ETSI TS 122 368, *Digital cellular telecommunications system (Phase 2+); Universal Mobile Telecommunications System (UMTS); LTE; Service requirements for Machine-Type Communications (MTC); Stage 1 (3GPP TS 22.368).*

3 Définitions

3.1 Termes définis ailleurs

La présente Recommandation utilise les termes suivants définis ailleurs:

3.1.1 entité d'application (AE) [UIT-T Y.4500.11]: instanciation de la logique d'application pour les solutions M2M de bout en bout.

3.1.2 entité de services communs (CSE) [UIT-T Y.4500.11]: instanciation d'un ensemble de fonctions de services communs des environnements M2M. Ces fonctions sont présentées aux autres entités via des points de référence.

3.2 Termes définis dans la présente Recommandation

Aucun.

4 Abréviations et acronymes

La présente Recommandation utilise les abréviations et acronymes suivants:

AE entité d'application (*application entity*)

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

CMDH gestion de la communication et de la fourniture (*communication management and delivery handling*)

CPU unité centrale de traitement (*central processing unit*)

DM gestion des dispositifs (*device management*)

GBA architecture d'amorçage générique (*generic bootstrapping architecture*)

GSMA Global System for Mobile Communications Association

GW passerelle (*gateway*)

HGI Home Gateway Initiative

HSM module matériel de sécurité (*hardware security module*)

IP protocole Internet (*Internet protocol*)

LWM2M protocole M2M simple (*lightweight M2M*)

M2M machine à machine *(machine to machine)*

MTC communications de type machine (*machine type communications*)

OMA Open Mobile Alliance

OSR exigences pour le système global (*overall system requirements*)

OWL langage d'ontologie web (*web ontology language*)

QoS qualité de service (*quality of service*)

RDF cadre de description des ressources (*resource description framework*)

SMS service de messages courts (*short message service*)

UICC carte à circuit intégré universelle (*universal integrated circuit card*)

USIM module d'identité d'abonné UMTS (*UMTS subscriber identity module*)

USSD données de service supplémentaire non structurées (*unstructured supplementary service data*)

WAN réseau étendu (*wide area network*)

WLAN réseau local sans fil (*wireless local area network*)

5 Conventions

Les mots clés "doit", "ne doit pas", "devrait", "ne devrait pas", "peut" et "n'a pas besoin" utilisés dans la présente Recommandation doivent être interprétés comme décrit ci-après:

Doit/ne doit pas:

Exigences

1) Effet pour la présente Recommandation: la Recommandation doit décrire la fonctionnalité requise (à savoir spécifier une solution technique pour l'exigence).
2) Effet pour les produits: chaque mise en oeuvre (solution M2M conforme à la norme) doit prendre en charge la fonctionnalité.
3) Effet pour les déploiements: chaque déploiement (service M2M fondée sur la norme) doit utiliser la fonctionnalité normalisée le cas échéant, faute de quoi, par exemple, des problèmes d'interopérabilité avec les autres services pourraient se poser.

Devrait/ne devrait pas:

Recommandation:

1) Effet pour la présente Recommandation: la Recommandation doit décrire une solution qui permet à la fonctionnalité d'être présente ou absente.

2) Effet pour les produits: une mise en oeuvre peut ou non prendre en charge la fonctionnalité; toutefois, la prise en charge est recommandée.

3) Effet pour les déploiements: un déploiement peut ou non utiliser la fonctionnalité; toutefois, l'utilisation est recommandée.

Peut/n'a pas besoin:

Permission/option:

1) Effet pour la présente Recommandation: la Recommandation doit décrire une solution qui permet à la fonctionnalité d'être présente ou absente.

2) Effet pour les produits: une mise en oeuvre peut ou non prendre en charge la fonctionnalité.

3) Effet pour les déploiements: un déploiement peut ou non utiliser la fonctionnalité.

6 Présentation de l'écosystème M2M

6.1 Description des rôles fonctionnels

La Figure 1 illustre les rôles fonctionnels dans l'écosystème de machine à machine (M2M).

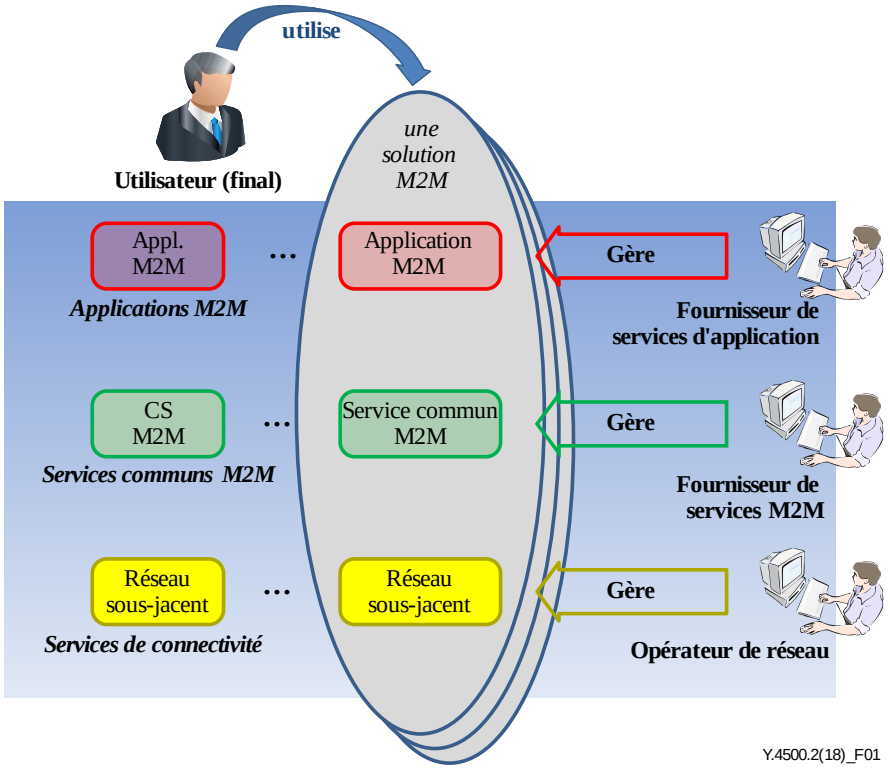

Figure 1 – Rôles fonctionnels dans l'écosystème M2M

1) L'*utilisateur* (individu ou société – autrement dit l'utilisateur final) remplit tous les critères suivants:

   – Utilise une solution M2M.

2) Le *fournisseur de services d'application* remplit tous les critères suivants:
   – Fournit un service d'application M2M.
   – Gère des applications M2M
3) Le *fournisseur de services M2M remplit tous les critères suivants:*
   – Fournit des services M2M aux fournisseurs de services d'application.
   – Gère des services communs M2M.
4) L'*opérateur de réseau* remplit tous les critères suivants:
   – Fournit des services de *connectivité* et des services connexes aux *fournisseurs de services M2M*.
   – Gère un *réseau sous-jacent*. Le réseau sous-jacent pourrait par exemple être un réseau de télécommunication.

Parmi les rôles fonctionnels ci-dessus, certains peuvent coïncider. Ces rôles fonctionnels n'impliquent pas de rôles opérationnels ou d'hypothèses relatives à l'architecture.

7 Exigences fonctionnelles (normatives)

7.1 Exigences pour le système global

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-001	Le système oneM2M doit permettre aux applications M2M de communiquer entre elles en utilisant plusieurs moyens de communication basés sur un accès utilisant le protocole Internet (IP).
OSR-002a	Le système oneM2M doit prendre en charge des moyens de communication adaptés aux dispositifs ayant des capacités limitées en termes de calculs (par exemple unité centrale de traitement (CPU), mémoire, batterie de faible capacité) ou de communications (par exemple modem sans fil 2G ou certains noeuds d'un réseau local hertzien (WLAN)).
OSR-002b	Le système oneM2M doit prendre en charge des moyens de communication adaptés aux dispositifs ayant des capacités importantes en termes de calculs (par exemple CPU, mémoire de grande capacité) ou de communications (par exemple modem sans fil 3/4G, système filaire).
OSR-003	Le système oneM2M doit permettre de maintenir des communications application-application en coordination avec une session d'application pour les applications M2M qui l'exigent.
OSR-004	Le système oneM2M doit prendre en charge des communications d'application en dehors de toute session pour les applications M2M qui l'exigent.
OSR-005	Le système oneM2M doit pouvoir présenter les services offerts par les réseaux de télécommunication aux applications M2M (par exemple service de messages courts (SMS), données de services supplémentaires non structurés (USSD), localisation, configuration d'abonnement, authentification (par exemple architecture d'amorçage générique), etc.), sous réserve des restrictions imposées par la politique de l'opérateur de réseau.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-006	Le système oneM2M doit pouvoir réutiliser les services offerts par les réseaux sous-jacents aux applications M2M et/ou les services M2M grâce à des modèles d'accès ouverts (par exemple OMA, cadre GSMA OneAPI). Comme exemples de services disponibles, on peut citer: • Communications multimédias IP. • Messagerie. • Emplacement. • Services de tarification et de facturation. • Informations sur les dispositifs et profils. • Configuration et gestion des dispositifs. • Déclenchement, contrôle des dispositifs. • Transmission d'une faible quantité de données. • Gestion de groupe. (voir la Note 1).
OSR-007	Le système oneM2M doit fournir un mécanisme permettant aux applications M2M d'interagir avec les applications et les données/informations gérées par un fournisseur de services M2M différent, sous réserve des permissions nécessaires.
OSR-008	Le système oneM2M doit permettre aux applications M2M de communiquer avec un dispositif M2M (à savoir une application dans le dispositif) sans nécessairement avoir connaissance de la technologie de réseau et du protocole de communication spécifique du dispositif M2M.
OSR-009	Le système oneM2M doit permettre à une ou plusieurs applications M2M d'interagir avec un ou plusieurs dispositifs/une ou plusieurs passerelles M2M (application dans le dispositif/la passerelle) (voir la Note 2).
OSR-010	Le système oneM2M doit prendre en charge des mécanismes permettant de confirmer la transmission d'un message à son destinataire pour les applications M2M demandant une transmission fiable afin de détecter tout échec de transmission de message dans un intervalle de temps donné.
OSR-011a	Le système oneM2M doit pouvoir demander des trajets de communication différents au réseau sous-jacent sur la base des politiques de l'opérateur du réseau sous-jacent et/ou du fournisseur de services M2M et des mécanismes de routage, en cas d'échecs de transmission.
OSR-011b	Le système oneM2M doit pouvoir demander des trajets de communication différents au réseau sous-jacent sur la base d'une demande émanant des applications M2M.
OSR-012	Le système oneM2M doit prendre en charge des communications entre des applications M2M et des dispositifs M2M prenant en charge des services M2M au moyen d'une connectivité continue ou non continue.
OSR-013	Le système oneM2M doit avoir connaissance de la tolérance de temps de transmission acceptable pour l'application M2M et doit planifier la communication en conséquence ou demander au réseau sous-jacent de le faire, sur la base des critères indiqués dans les politiques.
OSR-014	Le système oneM2M doit pouvoir communiquer avec les dispositifs M2M se trouvant derrière une passerelle M2M qui prend en charge des réseaux M2M hétérogènes.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-015	Le système oneM2M doit pouvoir aider les réseaux sous-jacents qui prennent en charge des schémas de communication différents, par exemple des communications peu fréquentes, le transfert de faibles quantités de données, le transfert de gros fichiers ou le streaming.
OSR-016	Le système oneM2M doit permettre aux applications M2M d'être informées au sujet des applications M2M disponibles/de la gestion au niveau des dispositifs/passerelles M2M, ainsi que des changements correspondants, en particulier des changements concernant le réseau M2M.
OSR-017	Le système oneM2M doit pouvoir offrir un accès à différents ensembles de services M2M aux fournisseurs d'applications M2M. L'ensemble de services minimal est le suivant: • Gestion de la connectivité. • Gestion des dispositifs (gestion au niveau du service). • Gestion des données d'application. Afin de permettre différents scénarios de déploiement, le système oneM2M doit mettre à disposition un seul de ces services, un sous-ensemble ou l'ensemble complet.
OSR-018	Le système oneM2M doit pouvoir offrir des services M2M aux dispositifs M2M en itinérance dans des réseaux sous-jacents cellulaires, sous réserve des restrictions imposées par la politique de l'opérateur de réseau (voir la Note 3).
OSR-019	Le système oneM2M doit prendre en charge les capacités de stockage de données (à savoir collecter/mémoriser) ainsi que de transfert de données depuis un ou plusieurs dispositifs M2M ou une ou plusieurs passerelles M2M à destination d'une ou plusieurs passerelles M2M, de l'infrastructure des services M2M ou de l'infrastructure des applications M2M, de la façon demandée par l'infrastructure des applications M2M comme listé ci-après: • action lancée par un dispositif M2M, une passerelle M2M, l'infrastructure des services M2M, ou l'infrastructure des applications M2M; • déclenchement selon un calendrier ou à la suite d'un événement; • pour des données spécifiées.
OSR-020	Le système oneM2M doit pouvoir prendre en charge des politiques et leur gestion en ce qui concerne les aspects de stockage et d'extraction des données/informations.
OSR-021	Le système oneM2M doit pouvoir fournir des mécanismes permettant de partager des données entre plusieurs applications M2M.
OSR-022	Lorsque certains composants d'une solution M2M ne sont pas disponibles (par exemple connexion WAN perdue), le système oneM2M doit pouvoir assurer le fonctionnement normal des composants de la solution M2M qui sont disponibles.
OSR-023	Le système oneM2M doit pouvoir identifier les services M2M à utiliser pour les abonnements aux services M2M (voir la Note 4).
OSR-024	Le système oneM2M doit pouvoir identifier les dispositifs M2M utilisés pour les abonnements aux services M2M.
OSR-025	Le système oneM2M doit pouvoir identifier les applications M2M utilisées pour les abonnements aux services M2M.
OSR-026	Si le réseau sous-jacent le permet, le système oneM2M doit pouvoir associer le dispositif M2M utilisé pour les abonnements aux services M2M avec les identifiants de dispositif offerts par le réseau sous-jacent et le dispositif.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-027	Le système oneM2M doit fournir un mécanisme générique permettant d'échanger de manière transparente des informations entre l'application M2M et le réseau sous-jacent, sous réserve des restrictions imposées par la politique du fournisseur de services M2M et/ou par la politique de l'opérateur de réseau (voir la Note 5).
OSR-028	Le système oneM2M doit permettre à une application M2M de définir des conditions de déclenchement dans le système oneM2M, afin que le système oneM2M envoie de façon autonome une série de commandes aux actionneurs au nom de l'application M2M lorsque ces conditions sont réunies.
OSR-029	Le système oneM2M doit pouvoir prendre en charge l'envoi d'une ou plusieurs commandes communes à chaque actionneur ou capteur via un groupe.
OSR-030	Le système oneM2M doit pouvoir prendre en charge la gestion (à savoir l'ajout, la suppression, l'extraction et la mise à jour) des membres d'un groupe.
OSR-031	Le système oneM2M doit pouvoir prendre en charge un groupe en tant que membre d'un autre groupe.
OSR-032	Le système oneM2M doit pouvoir prendre en charge des catégories d'événements (par exemple normal, urgent) associées aux données pour les applications M2M au moment de la collecte, du stockage et de la communication de ces données (voir la Note 6).
OSR-033	Sur la base du contexte dynamique du dispositif et/ou de la passerelle M2M et des catégories d'événements définies, le système oneM2M doit permettre d'ajuster dynamiquement la planification de l'envoi de rapports et de notifications pour le dispositif/la passerelle M2M (voir la Note 17).
OSR-034	Le système oneM2M doit prendre en charge le remplacement transparent des dispositifs et des passerelles M2M (par exemple reroutage du trafic, connexion, rétablissement, etc.).
OSR-035	Le système oneM2M doit prendre en charge l'échange d'informations pertinentes non liées aux applications M2M (par exemple classes de dispositif/passerelle) entre le dispositif/la passerelle M2M et l'infrastructure des services M2M afin d'améliorer l'efficacité des communications. En particulier, un dispositif M2M doit pouvoir signaler sa classe de dispositif à l'infrastructure des services M2M et l'infrastructure de services M2M doit pouvoir signaler ces capacités au dispositif M2M.
OSR-036	Le système oneM2M devrait fournir des mécanismes permettant d'accepter les demandes de services de calcul/d'analyse émanant des fournisseurs de services d'application M2M.
OSR-037	Le système oneM2M doit permettre à une application M2M de demander d'envoyer des données, indépendamment du réseau sous-jacent, aux applications M2M d'un groupe de dispositifs et de passerelles M2M se trouvant dans les zones géographiques spécifiées par l'application M2M.
OSR-038	Le système oneM2M doit prendre en charge l'inclusion de la préférence de QoS de l'application M2M dans les demandes de service aux réseaux sous-jacents.
OSR-039	Le système oneM2M doit pouvoir autoriser les demandes de service avec une préférence de QoS au niveau du service, mais doit transmettre la préférence de QoS de l'application M2M dans les demandes de service au réseau sous-jacent pour autorisation et acceptation ou négociation des demandes de QoS pour le service.
OSR-040	Le système oneM2M doit pouvoir tirer parti des multiples mécanismes de communication (par exemple USSD ou SMS) lorsqu'ils sont disponibles dans les réseaux sous-jacents.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-041	Le système oneM2M doit fournir un mécanisme qui prend en charge l'ajout de nouveaux services M2M dans le système oneM2M en tant que modules portables indépendants par le biais des interfaces oneM2M.
OSR-042	Le système oneM2M doit pouvoir prendre en charge différents niveaux de QoS en spécifiant des paramètres tels que le débit binaire garanti, le temps de transmission, la variation du temps de transmission, le taux de perte, le taux d'erreurs, etc.
OSR-043	Le système oneM2M doit pouvoir vérifier que les membres d'un groupe prennent en charge un ensemble commun de fonctions.
OSR-044	Le système oneM2M doit prendre en charge la communication avec les dispositifs M2M qui sont joignables selon un calendrier défini (par exemple périodiquement) ainsi qu'avec les dispositifs M2M qui sont joignables de manière imprévisible et spontanée.
OSR-045a	Le système oneM2M doit pouvoir recevoir et utiliser les informations fournies par le réseau sous-jacent concernant la question de savoir quand un dispositif M2M est joignable.
OSR-045b	Le système oneM2M doit pouvoir utiliser les calendriers de joignabilité générés par le dispositif M2M ou le domaine de l'infrastructure.
OSR-046	Le système oneM2M doit pouvoir permettre à une application M2M de demander/rejeter l'acquittement de ses communications.
OSR-047	Le système oneM2M doit pouvoir prendre en charge un mécanisme permettant aux dispositifs et/ou passerelles M2M de communiquer les informations relatives à leur emplacement géographique aux applications M2M (voir la Note 7).
OSR-048	Le système oneM2M doit fournir un service M2M qui permet aux dispositifs et/ou passerelles M2M de partager les informations relatives à leur propre emplacement géographique ou celles relatives à l'emplacement géographique d'autres dispositifs M2M (voir la Note 7).
OSR-049	Le système oneM2M doit pouvoir permettre à une application M2M de partager des données (par exemple contrôle d'accès) de manière sélective entre applications.
OSR-050	Si une communication sur un canal de communication fourni par le réseau sous-jacent ne peut être déclenchée que d'un côté (domaine de l'infrastructure ou domaine du champ), et qu'un ou plusieurs autres canaux sont disponibles dans l'autre sens, le système oneM2M doit pouvoir utiliser ces autres canaux pour déclencher une communication bidirectionnelle sur le premier canal.
OSR-051	Sous réserve de la disponibilité d'interfaces adaptées fournies par le réseau sous-jacent, le système oneM2M doit pouvoir demander au réseau sous-jacent de procéder à une diffusion générale/multidiffusion de données à un groupe de dispositifs M2M se trouvant dans une zone spécifiée.
OSR-052	Le système oneM2M doit pouvoir choisir un réseau sous-jacent approprié pour procéder à une diffusion générale/multidiffusion de données en fonction de la prise en charge de la diffusion générale/multidiffusion par le réseau et de la connectivité prise en charge par le groupe ciblé de dispositifs/passerelles M2M.
OSR-053	Le système oneM2M doit fournir un moyen d'assurer la rétrocompatibilité des interfaces entre les différentes versions (voir la Note 8).
OSR-054	Le système oneM2M doit pouvoir permettre à une application M2M, un dispositif M2M ou une passerelle M2M d'avoir accès aux ressources d'une autre application M2M, d'un autre dispositif M2M ou d'une autre passerelle M2M.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-055	Le système oneM2M doit pouvoir permettre aux applications M2M d'échanger des données avec une ou plusieurs applications M2M autorisées qui ne sont pas connues à l'avance.
OSR-056	Le système oneM2M doit permettre de découvrir les applications M2M utilisables au niveau d'une passerelle M2M ou d'un dispositif M2M.
OSR-057	Le système oneM2M doit permettre de découvrir les passerelles M2M et les dispositifs M2M accessibles par une application M2M pour l'échange de données.
OSR-058	Le système oneM2M doit pouvoir fournir les horodates requises par les fonctions de services communs.
OSR-059	Le système oneM2M doit pouvoir prendre en charge le contrôle d'accès fondé sur le rôle sur la base des abonnements aux services M2M.
OSR-060	Le système M2M devrait assurer une synchronisation temporelle avec une source d'horloge externe.
OSR-061	Les dispositifs et passerelles M2M peuvent assurer une synchronisation temporelle à l'intérieur du système oneM2M.
OSR-062	Le système oneM2M doit permettre de vérifier la connectivité pour un ensemble d'applications M2M.
OSR-063	Le système oneM2M doit pouvoir gérer la planification de la connectivité de la couche service M2M et de la messagerie entre le domaine de l'infrastructure et les dispositifs/passerelles M2M.
OSR-064	Le système oneM2M doit pouvoir regrouper les messages en fonction de la tolérance de temps de transmission des messages et/ou de leur catégorie.
OSR-065	Le système oneM2M doit fournir des mécanismes permettant à un fournisseur de services M2M de distribuer des fonctions de traitement à ses dispositifs/passerelles M2M dans le domaine du champ.
OSR-066	Le système oneM2M doit pouvoir prendre en charge la mise en place et l'exploitation d'applications M2M dans certains noeuds M2M selon les critères demandés par les fournisseurs de services d'application M2M, sous réserve des droits d'accès.
OSR-067	Le système oneM2M doit pouvoir exécuter les tâches opérationnelles et de gestion demandées par les applications M2M.
OSR-068	Lorsque le réseau sous-jacent le permet, le système oneM2M doit pouvoir offrir la capacité d'extraire et de communiquer les informations relatives à la question de savoir si un dispositif M2M est autorisé à accéder aux services de réseau sous-jacent.
OSR-069	Lorsque le réseau sous-jacent le permet, le système oneM2M doit pouvoir maintenir l'état opérationnel des services M2M pour un dispositif M2M et le mettre à jour lorsque l'état des services de connectivité du réseau sous-jacent change.
OSR-070	Le système oneM2M doit pouvoir offrir la capacité d'envoyer une notification à une application M2M autorisée lorsque l'état administratif ou l'état opérationnel des services M2M d'un dispositif M2M change, si cette application M2M s'est abonnée à ce type de notifications.
OSR-071	Le système oneM2M doit pouvoir permettre à une application M2M autorisée de définir l'état administratif des services M2M d'un dispositif M2M.
OSR-072	Le système oneM2M doit pouvoir lancer un ensemble de tâches bien définies (par exemple déclenchement à partir d'un seuil, comparaison de valeurs, etc.) concernant une ou plusieurs applications M2M au nom d'une autre application M2M.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-073	Le système oneM2M doit prendre en charge des transactions réparties entre plusieurs dispositifs ou applications lorsque la transaction présente les caractéristiques d'atomicité, de cohérence, d'isolement et de durabilité.
OSR-074	Le système oneM2M doit prendre en charge l'exécution de transactions réparties entre plusieurs dispositifs ou applications tout en maintenant l'ordre des opérations et en effectuant la transaction dans un laps de temps donné.
OSR-075	Le système oneM2M doit pouvoir collecter et stocker des séries de données chronologiques.
OSR-076	Le système oneM2M doit pouvoir détecter et signaler les données manquantes dans une série chronologique.
OSR-077	Le système oneM2M doit pouvoir collecter des réponses asynchrones se rapportant aux messages diffusées.
OSR-078	Le système oneM2M doit prendre en charge des capacités basées sur des passerelles pour la gestion des événements, par exemple la capacité d'arbitrage du traitement résultant.
OSR-079	Le système oneM2M doit permettre d'envoyer une notification à un dispositif hébergeant un groupe d'applications lorsque différents points d'enregistrement sont disponibles pour ce groupe d'applications (par exemple via différents réseaux sous-jacents) en fonction des exigences de service de chacune des applications hébergées.
OSR-080	Le système oneM2M doit permettre d'enregistrer les applications dans un groupe ou séparément, en fonctions des exigences de service associées.
OSR-081	Le système oneM2M doit pouvoir collecter les données qui sont diffusées (par exemple dans les systèmes de bus industriels) conformément aux politiques de collecte des données.
OSR-082	Le système oneM2M doit permettre de mettre à jour, de modifier ou de supprimer des politiques de collecte des données dans une application M2M.
OSR-083	Le système oneM2M doit pouvoir filtrer les informations émanant des dispositifs oneM2M pour un ensemble donné de paramètres.
OSR-084	Le système oneM2M doit pouvoir traiter une notification d'événement provenant d'une application M2M autorisée qui déclenche des tâches à exécuter au niveau du dispositif M2M (par exemple activer ou désactiver le contrôle).
OSR-085	Le système oneM2M doit prendre en charge la mise en mémoire cache des ressources des dispositifs M2M enregistrés. La mise en mémoire cache des ressources est un mécanisme par lequel le système oneM2M conserve les ressources d'un dispositif M2M enregistré dans un état d'inactivité temporaire en déplaçant les ressources vers une mémoire temporaire, par exemple un segment de mémoire cache.
OSR-086	Le système oneM2M doit permettre aux passerelles M2M de découvrir les noeuds d'infrastructure M2M et les dispositifs M2M disponibles pour l'échange de données.
OSR-087	Le système oneM2M doit permettre aux noeuds d'infrastructure M2M et aux dispositifs M2M de découvrir les passerelles M2M disponibles pour l'échange de données.
OSR-088	Le système oneM2M doit pouvoir prendre en charge les capacités de stockage de données (à savoir collecter/mémoriser) ainsi que de transfert de données parmi les dispositifs et passerelles M2M autorisés via des réseaux M2M, sans l'intervention du domaine de l'infrastructure.
OSR-089	Le système oneM2M doit permettre d'annuler la collecte de données en continu et/ou de supprimer des données collectées lorsque des conditions prédéfinies sont remplies.

Tableau 1 – Exigences pour le système global

Exigence	Description
OSR-090	Le système oneM2M doit pouvoir retransmettre les données d'application M2M à une application M2M sans stocker les données.
OSR-091	Le système oneM2M doit pouvoir envoyer une notification aux entités oneM2M intéressées lorsqu'il détecte que des données d'application M2M retransmises n'ont pas été transmises dans le délai prévu.
OSR-092	Le système oneM2M doit permettre de contrôler et de décrire les flux de données avec les attributs associés, par exemple actualité des données, précision, fréquence d'échantillonnage, intégrité des données.
OSR-093	Le système oneM2M doit prendre en charge la gestion des transactions pour plusieurs dispositifs ou applications avec un mécanisme basé sur des politiques qui devrait être invoqué (par exemple maintien de l'état, nouvelle planification, retour en arrière) en fonction des résultats de l'opération souhaitée.
OSR-094	Le système oneM2M doit fournir un ou plusieurs modèles d'information pour prendre en charge l'interopérabilité entre différents dispositifs/applications.
OSR-095	Le système oneM2M devrait fournir des mappages entre différents modèles d'information provenant d'un ou plusieurs systèmes autres que oneM2M.
OSR-096	Le système oneM2M devrait pouvoir interfonctionner avec des systèmes autres que oneM2M.
OSR-097	Le système oneM2M doit pouvoir partager des politiques de collecte des données entre plusieurs dispositifs/passerelles M2M dans le cadre d'un service d'application M2M, ou parmi différents services d'application M2M.
OSR-098	Le système oneM2M doit pouvoir prendre en charge des fonctionnalités de socialisation des machines (par exemple découverte de l'existence, découverte de tâches corrélées, découverte d'interface pour les messages et optimisation de processus pour plusieurs machines avec les mêmes tâches).
NOTE 1 – L'ensemble de fonctionnalités ou d'interfaces de programmation d'application (API) à prendre en charge dépend des services communs M2M et de l'accès aux interfaces API disponibles. NOTE 2 – La relation entre application de réseau M2M et dispositif/passerelle M2M peut être de type 1:1, 1:n, n:1 et/ou n:m. NOTE 3 – Pour cette exigence, on suppose qu'il n'y a pas d'itinérance au niveau des services M2M. NOTE 4 – Les abonnements aux services M2M ne sont pas des abonnements à des applications (par exemple gestion de l'énergie domestique). NOTE 5 – Pour l'échange transparent d'informations, on entend des informations qui sont principalement interprétées par l'application M2M et le fournisseur de réseau sous-jacent. NOTE 6 – Sur la base des catégories d'événements et grâce à l'interfonctionnement avec les réseaux sous-jacents, le système oneM2M peut prendre en charge des services différenciés (niveau de qualité de service) demandés par des applications M2M. NOTE 7 – Les informations relatives à l'emplacement géographique peuvent comprendre davantage d'informations que simplement la longitude, la latitude et les événements de géorepérage. NOTE 8 – Le terme "moyen" ne signifie pas uniquement des mécanismes techniques, par exemple il n'y a pas de négociation de la version du protocole. NOTE 9 – Dans la version 1, seules les fonctionnalités GBA et de localisation sont disponibles. NOTE 10 – La version 1 couvre: l'emplacement, les services de tarification et de facturation, la configuration et la gestion des dispositifs, les informations sur les dispositifs et les profils, le déclenchement.	

Tableau 1 – Exigences pour le système global

Exigence	Description
NOTE 11 – Cette exigence s'applique aux dispositifs M2M mais pas aux dispositifs en interfonctionnement via des réseaux M2M. NOTE 12 – Sur la base d'un déclenchement des dispositifs. NOTE 13 – Pas de prise en charge du streaming. NOTE 14 – Limitations concernant le déclenchement (via l'interface Tsp) des dispositifs dans un réseau visité. NOTE 15 – La syntaxe détaillée pour décrire le contexte dynamique n'est pas spécifiée. NOTE 16 – La transmission CoAP par SMS est possible, mais actuellement les interfaces de transmission de messages SMS ne sont pas définies explicitement. NOTE 17 – Par exemple, si la batterie de la passerelle n'est plus qu'à 10% ou moins, la passerelle notifie l'état à la plate-forme de services M2M. L'application M2M dans le noeud d'infrastructure ajustera la planification de l'envoi de rapports et de notifications sur la base des catégories d'événements associées à chaque message. Par conséquent, la passerelle M2M fonctionne plus longtemps. NOTE 18 – Vide. NOTE 19 – Seul l'état administratif des services M2M peut être notifié. L'état opérationnel des services M2M n'est pas mis en oeuvre. NOTE 20 – Une mise en oeuvre est possible sur la base des droits d'accès préconfigurés. NOTE 21 – Dans la version 1, la prise en charge est assurée au moyen des interfaces Mca, avec mappage du nouveau module de service avec une entité AE. NOTE 22 – Dans la version 2, les données sont stockées dans l'entité de services communs (CSE), mais ne sont jamais extraites par d'autres entités, sauf au moyen du mécanisme d'abonnement/notification.	

7.2 Exigences de gestion

Tableau 2 – Exigences de gestion

Exigence	Description
MGR-001	Le système oneM2M doit pouvoir prendre en charge la gestion et la configuration des passerelles/dispositifs M2M y compris des dispositifs M2M à ressources limitées.
MGR-002	Le système oneM2M doit permettre de découvrir les réseaux M2M y compris les informations concernant les dispositifs présents sur ces réseaux et les paramètres (par exemple topologie, protocole) de ces réseaux.
MGR-003	Le système oneM2M doit pouvoir permettre de maintenir et de décrire le modèle d'informations de gestion concernant les dispositifs et les paramètres (par exemple topologie, protocole) des réseaux M2M.
MGR-004	Le système oneM2M doit prendre en charge des moyens communs de gestion des dispositifs utilisant des technologies de gestion différentes (par exemple OMA DM, BBF TR069).
MGR-005	Le système oneM2M doit permettre de gérer plusieurs dispositifs de manière groupée.
MGR-006	Le système oneM2M doit permettre d'assurer la fourniture et la configuration des dispositifs dans les réseaux M2M.
MGR-007	Le système oneM2M doit permettre d'assurer le contrôle et le diagnostic des passerelles/dispositifs M2M dans les réseaux M2M.
MGR-008	Le système oneM2M doit permettre d'assurer la gestion logicielle des dispositifs dans les réseaux M2M.

Tableau 2 – Exigences de gestion

Exigence	Description
MGR-009	Le système oneM2M doit permettre d'assurer le redémarrage et/ou la réinitialisation des passerelles/dispositifs M2M et des autres dispositifs dans les réseaux M2M.
MGR-010	Le système oneM2M doit permettre d'assurer l'autorisation d'accès des dispositifs aux réseaux M2M.
MGR-011	Le système oneM2M doit permettre d'assurer la modification de la topologie des dispositifs dans les réseaux M2M, sous réserve des restrictions imposées par les politiques relatives au réseau M2M.
MGR-012	Dès qu'un nouveau dispositif est détecté, la passerelle M2M doit pouvoir être fournie par l'infrastructure de services M2M avec la configuration appropriée qui est nécessaire pour traiter le dispositif détecté.
MGR-013	Vide.
MGR-014	Le système oneM2M doit pouvoir extraire les événements et les informations journalisés par les passerelles/dispositifs M2M et les autres dispositifs dans les réseaux M2M.
MGR-015	Le système oneM2M doit pouvoir prendre en charge la gestion des micrologiciels (par exemple mise à jour) des passerelles/dispositifs M2M et des autres dispositifs dans les réseaux M2M.
MGR-016	Le système oneM2M doit pouvoir extraire les informations relatives au contexte statique et dynamique de dispositif/passerelle pour les passerelles/dispositifs M2M ainsi que le contexte de dispositif pour les autres dispositifs dans les réseaux M2M.
MGR-017	Le système oneM2M doit pouvoir corréler les éléments de gestion d'accès fournis par les protocoles de gestion de dispositif propres à une technologie avec les éléments de gestion d'accès utilisés par le système oneM2M.
MGR-018	L'infrastructure de services M2M doit pouvoir accepter les paramètres de configuration normalisés provenant d'un serveur de configuration externe pour permettre aux dispositifs M2M de s'enregistrer.
MGR-019	Le dispositif M2M doit pouvoir accepter les paramètres de configuration normalisés provenant d'un serveur de configuration externe afin de s'enregistrer sur le système oneM2M.
NOTE – Dans la version 1, il n'existe pas de mécanisme de détection, mais une fois qu'un dispositif M2M est connu au niveau de la passerelle, il peut être configuré via la passerelle grâce à la gestion de dispositif.	

7.3 Exigences relatives à la sémantique

7.3.1 Exigences relatives aux ontologies

Tableau 3 – Exigences relatives aux ontologies

Exigence	Description
ONT-001	Le système M2M doit prendre en charge un format normalisé pour les règles/politiques utilisées pour définir la logique de service.
ONT-002	Le système M2M doit prendre en charge la modélisation des descriptions sémantiques des objets (ainsi que des relations entre eux) au moyen d'ontologies.
ONT-003	Le système M2M doit prendre en charge un langage de modélisation commun pour les ontologies (par exemple OWL).

Tableau 3 – Exigences relatives aux ontologies

Exigence	Description
ONT-004	Le système M2M devrait pouvoir fournir des capacités de traduction depuis différents langages de modélisation des ontologies vers le langage adopté par le système oneM2M si la capacité d'expression de l'ontologie importée le permet.
ONT-005	Le système M2M doit permettre d'extraire les descriptions sémantiques et les ontologies stockées en dehors du système M2M.
ONT-006	Le système M2M doit permettre de relier les ontologies définies dans le contexte du système M2M avec les ontologies définies en dehors de ce contexte.
ONT-007	Le système M2M doit pouvoir prendre en charge l'extension des ontologies dans le système M2M.
ONT-008	Le système M2M doit pouvoir utiliser des ontologies qui renferment des concepts représentant des aspects (par exemple une salle) qui ne sont pas représentés par des ressources du système M2M.
ONT-009	Le système M2M doit pouvoir réutiliser des ontologies communes (par exemple ontologies pour l'emplacement, le temps, etc.) qui sont couramment utilisées dans les applications M2M.
ONT-010	Le système M2M doit pouvoir prendre en charge l'utilisation simultanée de multiples ontologies pour la même ressource M2M.
ONT-011	Le système M2M doit pouvoir rendre accessible une ontologie dans le système M2M, par exemple par le biais d'une annonce.
ONT-012	Le système M2M doit pouvoir prendre en charge des mécanismes permettant d'importer des ontologies extérieures dans le système M2M.
ONT-013	Le système M2M doit pouvoir assurer la mise à jour des ontologies.
ONT-014	Le système M2M doit offrir des fonctions de conversion des données sur la base d'ontologies.
ONT-015	Le système M2M doit pouvoir modéliser des dispositifs sur la base d'ontologies susceptibles d'être accessibles en dehors du système M2M (par exemple gabarit de dispositif HGI).
ONT-016	Le système M2M doit prendre en charge le stockage, la gestion et la découverte des ontologies.
ONT-017	Le système oneM2M doit prendre en charge une relation sémantique ("est apparié à") entre deux dispositifs M2M.

7.3.2 Exigences relatives aux annotations sémantiques

Tableau 4 – Exigences relatives aux annotations sémantiques

Exigence	Description
ANN-001	Le système oneM2M doit permettre de gérer les informations sémantiques relatives aux ressources oneM2M, par exemple créer, extraire, mettre à jour, supprimer, associer/relier.
ANN-002	Le système oneM2M doit prendre en charge un langage commun pour la description sémantique, par exemple le cadre de description des ressources (RDF).
ANN-003	Le système oneM2M doit prendre en charge l'annotation sémantique des ressources oneM2M, par exemple des données relatives aux applications figurant dans des conteneurs.

Tableau 4 – Exigences relatives aux annotations sémantiques

Exigence	Description
ANN-004	Le système oneM2M doit prendre en charge l'annotation sémantique basée sur des ontologies connexes.
ANN-005	Le système oneM2M doit pouvoir rendre accessibles les descriptions sémantiques dans le système M2M, par exemple par le biais d'une annonce.
ANN-006	Le système oneM2M doit permettre aux applications d'extraire une représentation ontologique liée à des informations sémantiques utilisées dans le système M2M.
ANN-007	Le système oneM2M doit permettre de gérer les descriptions de la qualité des données relatives à une ressource.

7.3.3 Exigences relatives aux interrogations sémantiques

Tableau 5 – Exigences relatives aux interrogations sémantiques

Exigence	Description
QRY-001	Le système oneM2M doit permettre de découvrir des ressources M2M sur la base de descriptions sémantiques.

7.3.4 Exigences relatives aux mixages sémantiques

Tableau 6 – Exigences relatives aux mixages sémantiques

Exigence	Description
MSH-001	Le système oneM2M doit permettre d'héberger des fonctions de traitement pour le mixage.
MSH-002	Le système oneM2M doit permettre aux applications M2M de fournir des fonctions de traitement pour le mixage.
MSH-003	Le système oneM2M proprement dit peut offrir des fonctions de traitement fournies préalablement ou créées dynamiquement pour le mixage.
MSH-004	Le système oneM2M doit pouvoir créer et exécuter des mixages sur la base des fonctions de traitement.
MSH-005	Le système oneM2M doit pouvoir présenter des mixages en tant que ressources, par exemple des dispositifs virtuels.

7.3.5 Exigences relatives aux raisonnements sémantiques

Tableau 7 – Exigences relatives aux raisonnements sémantiques

Exigence	Description
RES-001	Le système oneM2M doit pouvoir mettre à jour les ontologies sur la base d'un raisonnement ontologique.
RES-002	Le système oneM2M doit pouvoir prendre en charge un raisonnement sémantique, par exemple un raisonnement ontologique ou un raisonnement basé sur des règles sémantiques.
RES-003	Le système oneM2M doit pouvoir assurer l'ajout ou la mise à jour d'informations sémantiques sur la base d'un raisonnement sémantique.

7.3.6 Exigences relatives aux analyses de données

Tableau 8 – Exigences relatives aux analyses de données

Exigence	Description
ANA-001	Le système oneM2M doit pouvoir prendre en charge des capacités (par exemple une fonction de traitement) permettant d'effectuer des analyses de données M2M sur la base de descriptions sémantiques émanant d'applications M2M et/ou du système M2M.
ANA-002	Le système oneM2M doit permettre d'interpréter et d'appliquer une logique de service (par exemple des règles/politiques pour le déclenchement d'opérations sur d'autres ressources ou attributs lorsque la ressource contrôlée change) décrite au moyen d'une annotation sémantique et d'une ontologie.
ANA-003	Le système oneM2M doit prendre en charge un format normalisé pour les règles/politiques utilisées pour définir la logique de service.

7.4 Exigences relatives à la sécurité

Tableau 9 – Exigences relatives à la sécurité

Exigence	Description
SER-001	Le système M2M doit intégrer une protection contre les menaces ciblant sa disponibilité, par exemple les attaques par déni de service.
SER-002	Le système oneM2M doit pouvoir garantir la confidentialité des données.
SER-003	Le système oneM2M doit pouvoir garantir l'intégrité des données.
SER-004	Dans le cas où les dispositifs M2M prennent en charge un module d'identité d'abonné UMTS (USIM) sur une carte à circuit intégré universelle (UICC) contenant et les réseaux sous-jacents assurent la sécurité dans la couche réseau, le système oneM2M doit pouvoir tirer parti des justificatifs USIM/UICC des dispositifs et de la capacité de sécurité du réseau, par exemple 3GPP GBA, pour établir la sécurité au niveau des services et applications M2M par le biais d'interfaces avec le réseau sous-jacent.
SER-005	Dans le cas où les dispositifs M2M prennent en charge une carte USIM/UICC et les réseaux sous-jacents assurent la sécurité dans la couche réseau, et lorsque le système oneM2M a connaissance de la capacité d'amorçage du réseau sous-jacent, par exemple 3GPP GBA, le système oneM2M doit pouvoir présenter cette capacité aux services et applications M2M par le biais d'une interface API.
SER-006	Dans le cas où les dispositifs M2M prennent en charge une carte USIM/UICC et les réseaux sous-jacents assurent la sécurité dans la couche réseau, le système oneM2M doit pouvoir tirer parti des justificatifs USIM/UICC des dispositifs lorsqu'ils sont disponibles pour amorcer l'association de sécurité M2M.
SER-007	Lorsque certains composants d'une solution M2M ne sont pas disponibles (par exemple connexion WAN perdue), le système oneM2M doit pouvoir assurer la confidentialité et l'intégrité des données entre les composants autorisés de la solution M2M qui sont disponibles.
SER-008	Le système oneM2M doit prendre en charge des mesures de protection contre l'accès non autorisé aux services M2M et services d'application M2M.
SER-009	Le système oneM2M doit pouvoir assurer une authentification mutuelle pour l'interaction avec les réseaux sous-jacents, les services M2M et les services d'application M2M.
SER-010	Le système oneM2M doit pouvoir prendre en charge des mécanismes de protection contre l'utilisation abusive, le clonage, la substitution ou le vol de justificatifs de sécurité.

Tableau 9 – Exigences relatives à la sécurité

Exigence	Description
SER-011	Le système M2M doit protéger l'utilisation de l'identité d'une partie prenante M2M dans le système oneM2M contre la découverte et l'utilisation abusive par d'autres parties prenantes.
SER-012	Le système oneM2M doit pouvoir prendre en charge des mesures de protection contre les attaques par usurpation d'identité et les attaques par répétition.
SER-013	Le système oneM2M doit pouvoir prendre en charge un mécanisme de vérification de l'intégrité lors du démarrage, périodiquement en cours d'exécution et lors des mises à jour logicielles des composants logiciels/matériels/micrologiciels des dispositifs M2M.
SER-014	Le système oneM2M doit pouvoir fournir les données de configuration à une application M2M authentifiée et autorisée dans la passerelle/le dispositif M2M.
SER-015	Le système oneM2M doit pouvoir prendre en charge des mécanismes permettant de fournir l'identité de l'abonné à un service M2M aux applications M2M authentifiées et autorisées lorsque le système oneM2M a l'accord de l'abonné au service M2M.
SER-016	Le système oneM2M doit pouvoir assurer la non-répudiation à l'intérieur de la couche service M2M et pour ses interactions autorisées avec les couches réseau et application.
SER-017	Le système oneM2M doit pouvoir atténuer les menaces. NOTE – Des exemples de menaces sont recensés dans le rapport [b-oneM2M TR-0008].
SER-018	Le système oneM2M doit permettre à une partie prenante M2M d'utiliser une ressource ou un service et d'être responsable de cette utilisation sans divulguer son identité aux autres parties prenantes.
SER-019	Le système oneM2M doit pouvoir utiliser les justificatifs au niveau du service présents à l'intérieur du dispositif M2M pour établir la sécurité au niveau des services M2M et applications M2M.
SER-020	Le système oneM2M doit permettre aux fournisseurs de services M2M légitimes de fournir leurs propres justificatifs dans les dispositifs/passerelles M2M.
SER-021	Le système oneM2M doit pouvoir fournir à distance et en toute sécurité les justificatifs de sécurité M2M dans les dispositifs M2M et/ou les passerelles M2M.
SER-022	Le système oneM2M doit permettre aux fournisseurs de services d'application M2M d'autoriser les interactions mettant en jeu leurs applications M2M au niveau d'entités support (par exemple dispositifs/passerelles/infrastructure des services).
SER-023	Lorsqu'un module matériel de sécurité (HSM) est pris en charge, le système oneM2M doit pouvoir faire appel au module HSM pour assurer la sécurité locale.
SER-024	Le système oneM2M doit permettre aux applications M2M d'utiliser des environnements de sécurité différents et séparés.
SER-025	Le système oneM2M doit pouvoir empêcher les parties prenantes M2M non autorisées d'identifier et/ou d'observer les actions des autres parties prenantes M2M dans le système oneM2M, par exemple l'accès aux ressources et aux services (voir la Note 1).
SER-026	Le système oneM2M doit pouvoir fournir un mécanisme de protection de la confidentialité des informations relatives à l'emplacement géographique (voir la Note 2).
SER-027	Le système M2M doit prendre en charge le regroupement des applications M2M qui ont les mêmes droits de contrôle d'accès vers un même ensemble de ressources spécifique, de manière à ce que le contrôle d'accès puisse être validé en validant le fait que l'application M2M appartient à un certain groupe.

Tableau 9 – Exigences relatives à la sécurité

Exigence	Description
SER-028	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de données générées par une application individuelle afin que les entités intermédiaires (fiables ou non fiables) retransmettant les données ne puissent pas accéder aux portions protégées des données en clair.
SER-029	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de données générées par une application individuelle afin que les points d'extrémité du protocole de sécurité puissent détecter toute modification, y compris toute modification par des entités intermédiaires de la couche service (fiables ou non fiables) retransmettant les données.
SER-030	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de messages oneM2M individuels afin que les entités intermédiaires (fiables ou non fiables) retransmettant les messages ne puissent pas accéder aux portions protégées des messages en clair.
SER-031	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de messages oneM2M individuels afin que les points d'extrémité du protocole de sécurité puissent détecter toute modification, y compris toute modification par des entités intermédiaires de la couche service (fiables ou non fiables) retransmettant les messages.
SER-032	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité d'établir des sessions de sécurité qui sont utilisées pour protéger des portions d'un ou plusieurs messages oneM2M afin que les entités intermédiaires (fiables ou non fiables) retransmettant les messages ne puissent pas accéder aux portions protégées des messages en clair.
SER-033	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité d'établir des sessions de sécurité qui sont utilisées pour protéger des portions d'un ou plusieurs messages oneM2M afin que les points d'extrémité du protocole de sécurité puissent détecter toute modification, y compris toute modification par des entités intermédiaires de la couche service (fiables ou non fiables) retransmettant les messages.
SER-034	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de messages ou de données afin que les entités intermédiaires (fiables ou non fiables) retransmettant les messages ou les données ne puissent pas accéder aux portions protégées des messages ou données en clair.
SER-035	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de protéger des portions de messages ou de données afin que les points d'extrémité du protocole de sécurité puissent détecter toute modification, y compris toute modification par des entités intermédiaires de la couche service (fiables ou non fiables) retransmettant les messages ou les données.
SER-036	Le système oneM2M doit permettre aux points d'extrémité du protocole de sécurité de s'authentifier mutuellement sans faire appel à des entités intermédiaires de la couche service (fiables ou non fiables).
SER-037	Le système oneM2M doit pouvoir prendre en charge des fonctions d'autorisation réparties aux fins de la prise de décisions en matière de contrôle d'accès, de la fourniture de politiques de contrôle d'accès et de la fourniture d'attributs d'autorisation (par exemple rôles).
SER-038	Le système oneM2M doit pouvoir présenter une interface interopérable pour fournir des politiques de contrôle d'accès au moyen du langage spécifié pour les politiques de contrôle d'accès.

Tableau 9 – Exigences relatives à la sécurité

Exigence	Description
SER-039	Le système oneM2M doit permettre aux individus d'établir des politiques pour le contrôle d'accès à leurs informations d'identification personnelle, y compris dans le cas où ces informations auraient été recueillies à leur insu.
SER-040	Lorsque les dispositifs M2M sont regroupés et que la passerelle M2M est autorisée en tant que déléguée du groupe à accéder au serveur M2M, la passerelle M2M doit pouvoir, au nom des dispositifs M2M du groupe, effectuer une authentification mutuelle avec le serveur M2M.
SER-041	Lorsque les dispositifs M2M sont regroupés et que la passerelle M2M appartient à un tiers, le système oneM2M doit pouvoir protéger la sécurité et la confidentialité des communications entre chaque dispositif M2M et le serveur M2M vis-à-vis des autres dispositifs M2M et de la passerelle M2M tierce.
SER-042	Une interface API sécurisée doit permettre aux entités de la couche application et de la couche service d'utiliser des fonctions et des données sensibles résidant dans l'environnement sécurisé, indépendamment de la mise en oeuvre technique de l'environnement sécurisé.
SER-043	Le système oneM2M doit permettre d'autoriser une entité oneM2M à déléguer temporairement ses droits d'accès (ou un sous-ensemble) à une autre entité oneM2M autorisée, mais les droits d'accès délégués dynamiquement ne doivent pas permettre à l'entité oneM2M délégataire de déléguer à son tour les mêmes droits à une troisième entité oneM2M.
SER-044	En ce qui concerne des données de service d'application M2M qui sont traitées par une application M2M B dans une entité M2M (par exemple passerelle M2M) se trouvant entre l'expéditeur A et l'application M2M destinataire C, le système oneM2M doit fournir un moyen permettant au destinataire de vérifier: • l'intégrité des données reçues par l'application M2M B en provenance de l'expéditeur A; et, dans le même temps: • l'absence de dysfonctionnement au niveau de l'application M2M B qui a traité les données.
SER-045	Le système oneM2M doit prendre en charge le classement des données d'application par les applications M2M selon divers niveaux de sécurité qui sont spécifiés par le système oneM2M et prendre en charge le mappage de ces niveaux vers les capacités de sécurité applicables.
SER-046	Le système oneM2M doit permettre d'assurer la protection de l'intégrité et l'authentification du créateur pour ce qui est des portions de données générées par une application individuelle qui sont en mémoire (par exemple données hébergées).
SER-047	Le système oneM2M doit permettre d'assurer la protection de la confidentialité pour ce qui est des portions de données générées par une application individuelle qui sont en mémoire (par exemple données hébergées).
SER-048	Le système M2M doit garantir que les justificatifs pour les données de bout en bout bénéficient d'une protection de la confidentialité et de l'intégrité et sont protégés contre toute falsification.
SER-049	Le système M2M doit garantir que les justificatifs pour les données de bout en bout sont protégés contre toute divulgation aux entités intermédiaires.
SER-050	Le système oneM2M doit permettre de protéger les conditions prédéfinies contre toute modification non autorisée.

Tableau 9 – Exigences relatives à la sécurité

Exigence	Description
SER-051	Le système oneM2M doit permettre de supprimer des données M2M produites/stockées par les dispositifs/passerelles M2M sur demande d'une entité autorisée.
SER-052	Le système oneM2M doit stocker et traiter les préférences en matière de confidentialité de manière interopérable.
SER-053	Le système oneM2M doit prendre en charge des profils de confidentialité à divers niveaux pour tenir compte des conditions liées aux dispositions juridiques, aux fabricants et aux personnes.
SER-054	Le système oneM2M doit pouvoir prioriser les profils de confidentialité en cas de conflits entre profils (par exemple le profil juridique est prioritaire par rapport au profil de la personne).
SER-055	Le système oneM2M doit pouvoir permettre à un utilisateur disposant de privilèges de configurer les paramètres liés à la sécurité de ses composants côté infrastructure par le biais d'une interface API normalisée.
SER-056	Le système oneM2M doit permettre à un utilisateur disposant de privilèges d'annuler et remplacer des paramètres de sécurité par le biais d'une interface API normalisée.
SER-057	Le système oneM2M doit prendre en charge un mécanisme permettant d'ajouter/de supprimer des informations pour l'authentification des entités oneM2M par le biais d'une interface API normalisée.
SER-058	Le système oneM2M doit permettre de déléguer les fonctions de sécurité (par exemple authentification/protection de l'intégrité des messages) d'une entité à une entité digne de confiance.
SER-059	Le système M2M doit protéger l'authenticité, l'intégrité et la confidentialité de la représentation des droits d'accès délégués.
SER-060	Le système oneM2M doit pouvoir révoquer la représentation des droits d'accès délégués.
SER-061	Le système oneM2M doit pouvoir vérifier l'identifiant de l'application à l'appui de toute détection de l'usurpation d'identité ou de toute révocation.
SER-062	Le système oneM2M doit pouvoir réutiliser la politique de confidentialité du réseau sous-jacent.
SER-063	Le système oneM2M doit pouvoir partager sa politique de confidentialité avec le réseau sous-jacent.
NOTE 1 – L'exigence ci-dessus ne s'applique pas aux éléments à l'extérieur du système oneM2M, par exemple les réseaux sous-jacents. NOTE 2 – Les informations relatives à l'emplacement géographique peuvent comprendre davantage d'informations que simplement la longitude et la latitude. NOTE 3 – Prise en charge partielle pour les attaques par usurpation d'identité, pas de prise en charge pour les attaques par répétition. NOTE 4 – Le système oneM2M ne dispose d'aucun moyen pour vérifier l'accord d'un abonné. Cette exigence ne peut être respectée qu'au niveau application. NOTE 5 – En ce qui concerne la fourniture à distance, la version 1 prend en charge uniquement la fourniture à distance des justificatifs pour les clés symétriques.	

7.5 Exigences relatives à la tarification

Tableau 10 – Exigences relatives à la tarification

Exigence	Description
CHG-001	Le système oneM2M doit prendre en charge la collecte d'informations de tarification relatives aux différents services offerts grâce au système oneM2M (par exemple gestion des données, gestion des dispositifs et/ou gestion de la connectivité). La collecte d'informations de tarification doit pouvoir se faire en même temps que l'utilisation des ressources. Le format des informations enregistrées doit être entièrement spécifié, y compris les éléments obligatoires et facultatifs.
CHG-002	Le système oneM2M doit prendre en charge des mécanismes propres à faciliter la corrélation des informations de tarification (par exemple d'un utilisateur) collectées pour les services M2M, les services d'application M2M et les services fournis par les opérateurs de réseau sous-jacent.
CHG-003	Le système oneM2M doit fournir un moyen permettant de coordonner les relevés de données de tarification correspondant aux données d'utilisation avec une qualité de service différenciée offerte par le réseau sous-jacent.
CHG-004	Le système oneM2M doit pouvoir utiliser les mécanismes de tarification existants des réseaux sous-jacents.
CHG-005	Le système oneM2M doit prendre en charge le transfert des relevés de données de tarification au domaine de facturation du fournisseur de services M2M, aux fins de: • la facturation de l'abonné; • la facturation entre fournisseurs; • la comptabilité fournisseur-abonné, y compris des fonctions additionnelles comme les statistiques.
CHG-006	Le système M2M devrait prendre en charge la génération d'événements de tarification afin de demander une autorisation d'utilisation de ressources auprès du système de contrôle de crédit en temps réel dont relève le compte de l'abonné. Les informations contenues dans les événements de tarification et les événements facturables correspondants doivent être entièrement spécifiées, y compris les éléments obligatoires et facultatifs (voir la Note 1).
NOTE 1 – On entend par événement facturable toute activité qui utilise les ressources et les services M2M connexes offerts par un fournisseur et que ledit fournisseur peut souhaiter facturer. On entend par événement de tarification l'ensemble des informations de tarification dont a besoin le système de contrôle de crédit pour l'autorisation des ressources. NOTE 2 – Les informations collectées peuvent être envoyées aux réseaux sous-jacents qui peuvent les utiliser pour la tarification. NOTE 3 – La couche service oneM2M peut transmettre les informations aux réseaux sous-jacents mais ne peut pas utiliser de mécanisme de réseau sous-jacent. La tarification peut être faite par le réseau sous-jacent. Ceci fait l'objet de l'exigence CHG-002. NOTE 4 – Prise en charge uniquement dans le noeud d'infrastructure.	

7.6 Exigences opérationnelles

Tableau 11 – Exigences opérationnelles

Exigence	Description
OPR-001	Le système oneM2M doit permettre d'assurer le contrôle et le diagnostic des applications M2M.
OPR-002	Le système oneM2M doit permettre d'assurer la gestion logicielle des applications M2M.
OPR-003	Le système oneM2M doit pouvoir configurer l'état d'exécution d'une application M2M (démarrage, arrêt, redémarrage).
OPR-004	Lorsque des interfaces adaptées sont fournies par le réseau sous-jacent, le système M2M doit pouvoir planifier le trafic via le réseau sous-jacent sur la base des instructions reçues du réseau sous-jacent.
OPR-005	Le système oneM2M doit pouvoir échanger avec les applications M2M des informations relatives aux caractéristiques d'utilisation et de trafic des dispositifs M2M ou des passerelles M2M concernant les applications M2M. La fonctionnalité 3GPP dite de temporisation [ETSI TS 122 368] devrait être prise en charge (voir la Note).
OPR-006	En fonction de la disponibilité d'interfaces adaptées fournies par le réseau sous-jacent, le système oneM2M doit pouvoir fournir des informations relatives aux caractéristiques d'utilisation et de trafic des dispositifs M2M ou des passerelles M2M au réseau sous-jacent.
OPR-007	Le système oneM2M doit pouvoir assurer la réception des informations d'état du réseau sous-jacent en cas de prise en charge par le réseau sous-jacent.
OPR-008	Le système oneM2M doit pouvoir fournir aux applications M2M les informations d'état reçues du réseau sous-jacent.
OPR-009	Le format des identifiants d'application enregistrés doit être tel qu'il soit facile pour les personnes et les systèmes de savoir si un identifiant d'application est enregistré et de déterminer l'autorité d'enregistrement qui a délivré l'identifiant, le développeur de l'application et le nom de l'application.
OPR-010	Les autorités d'enregistrement du système oneM2M doivent pouvoir collecter et conserver les informations d'accompagnement requises lors de l'attribution d'un identifiant d'application.
NOTE – La fonctionnalité de temporisation est équivalente aux fonctionnalités MTC spécifiées au § 7.2 de la spécification [ETSI TS 122 368].	

7.7 Exigences relatives à la gestion des communications

Tableau 12 – Exigences relatives à la gestion des communications

Exigence	Description
CMR-001	Le système oneM2M doit fournir aux applications M2M un service de communication qui assure la mise en mémoire tampon des messages à destination/en provenance de la passerelle/du dispositif M2M/du domaine de l'infrastructure.
CMR-002	Le système oneM2M doit pouvoir prendre en charge la retransmission des messages mis en mémoire tampon en fonction des politiques de communication et sur la base de la préférence de service associée aux messages mis en mémoire tampon.

Tableau 12 – Exigences relatives à la gestion des communications

Exigence	Description
CMR-003	Le système oneM2M doit permettre à une application M2M d'envoyer une demande de communication incluant la préférence de service comme suit: • paramètres de QoS, y compris la tolérance de temps de transmission, pour lancer la transmission des données; • classement de la demande de communication selon différents niveaux de priorité ou classes de QoS.
CMR-004	Le système oneM2M doit pouvoir assurer le traitement simultané au sein des passerelles M2M et/ou des dispositifs M2M de messages provenant de différentes sources compte tenu de la préférence de service associée aux messages tout en respectant les politiques de communication fournies.
CMR-005	Le système oneM2M doit pouvoir maintenir le contexte associé aux sessions M2M (par exemple le contexte de sécurité ou le contexte de connectivité de réseau pendant l'interruption de la session).
CMR-006	Le système oneM2M doit permettre aux applications de classer les communications demandées (priorité, importance, etc.), afin que le système oneM2M puisse adapter ses communications effectives (planification, regroupement, compression, etc.) en tenant compte de ce classement.
CMR-007	Le système oneM2M doit prendre en charge des politiques de communication configurables qui définiront ses schémas de communication. Ces politiques doivent tenir compte des informations reçues du réseau sous-jacent (par exemple les informations visées dans l'exigence OPR-004) ainsi que des informations reçues des applications (par exemple les informations visées dans l'exigence OPR-005 ou le classement des communications demandées par les applications).
CMR-008	Le système oneM2M doit prendre en charge le regroupement des données sur la base des politiques de communication lors de l'échange de données entre passerelle/dispositif M2M/domaine de l'infrastructure.
CMR-009	Le système M2M devrait prendre en charge la compression des données sur la base des politiques de communication lors de l'échange de données entre passerelle/dispositif M2M/domaine de l'infrastructure.
CMR-010	Le système oneM2M doit prendre en charge un temps de transmission aléatoire supplémentaire des communications, sur la base des politiques de communication, lors de l'échange de données entre passerelle/dispositif M2M/domaine de l'infrastructure.
CMR-011	Le système oneM2M doit pouvoir contrôler sa propre utilisation des réseaux sous-jacents sur des périodes données: tentatives de communications, tentatives infructueuses et tentatives fructueuses.
CMR-012	Le système oneM2M doit pouvoir limiter sa propre utilisation des réseaux sous-jacents, sur la base des politiques de communication et du contrôle de cette utilisation qu'il effectue, lors de l'échange de données entre passerelle/dispositif M2M domaine de l'infrastructure.
CMR-013	Le système oneM2M doit pouvoir s'abstenir d'utiliser les réseaux sous-jacents, sur la base d'une procédure de repli temporel configurable dans les politiques de communication, lors de l'échange de données entre passerelle/dispositif M2M/domaine de l'infrastructure.

Tableau 12 – Exigences relatives à la gestion des communications

Exigence	Description
CMR-014	Le système oneM2M doit pouvoir limiter sa propre utilisation des réseaux sous-jacents, sur la base des politiques de communication ainsi que de la date et de l'heure, lors de l'échange de données entre passerelle/dispositif M2M/domaine de l'infrastructure.
CMR-015	Le système oneM2M doit pouvoir identifier une série de données (par exemple série de données chronologiques) et indiquer des données individuelles appartenant à cette série.
NOTE 1 – L'enregistrement et le contexte de sécurité de longue durée sont couverts, les sessions M2M ne sont pas couvertes. NOTE 2 – Les politiques de gestion de la communication et de la fourniture [CMDH (côté application)] sont mises en oeuvre, les informations provenant du réseau sous-jacent peuvent être utilisées mais la méthode de fourniture via Mcn n'est pas couverte.	

7.8 Exigences relatives à l'interfonctionnement LWM2M

Tableau 13 – Exigences relatives à l'interfonctionnement LWM2M

Exigence	Description
LWM2M-001	Le système oneM2M doit permettre de transporter de façon transparente des objets LWM2M entre clients LWM2M et applications M2M.
LWM2M-002	Le système oneM2M doit permettre de convertir des objets LWM2M sous la forme d'une représentation sémantique en tant que ressources oneM2M.
LWM2M-003	Le système oneM2M doit fournir au serveur LWM2M des capacités d'interfonctionnement entre clients LWM2M et applications M2M.
LWM2M-004	Le système oneM2M doit permettre aux applications M2M de découvrir des clients LWM2M en utilisant le nom de point d'extrémité correspondant.
LWM2M-005	Lors du transport transparent d'objets LWM2M, le système oneM2M doit permettre aux applications M2M de découvrir la définition des objets LWM2M transportés par le système oneM2M.
LWM2M-006	Lors de l'interfonctionnement avec des objets LWM2M, le système oneM2M doit permettre aux applications M2M de découvrir un objet LWM2M en utilisant son identifiant.
LWM2M-007	Le système oneM2M doit permettre de prendre en charge des dispositifs qui incorporent un client LWM2M.
LWM2M-008	Le système oneM2M doit permettre d'assurer un interfonctionnement entre les mécanismes de sécurité sous-jacents du client LWM2M et les capacités de sécurité fournies par le système oneM2M.

8 Exigences non fonctionnelles (informatives)

La présente section vise à rassembler des principes et des lignes directrices de haut niveau régissant la conception du système oneM2M. Ces principes et lignes directrices sont fondamentaux pour la conception du système oneM2M. Mais comme ils ne peuvent pas nécessairement être exprimés intrinsèquement sous la forme d'exigences, ils sont exposés dans la présente section.

Tableau 14 – Exigences non fonctionnelles

Exigence	Description
NFR-001	La Continua Health Alliance incorpore une approche RESTful dans ses directives de conception. Pour prendre en charge ces directives, il convient, pour le système oneM2M, de prendre en considération les styles et approches RESTful lors de la conception de l'architecture M2M.
NFR-002	Le système oneM2M devrait communiquer au moyen de protocoles qui sont efficaces en termes de quantité d'informations échangées/quantité de données échangées mesurées en octets.

Annexe A

Procédure à suivre concernant l'actualisation et la tenue à jour des spécifications oneM2M

(Cette annexe fait partie intégrante de la présente Recommandation.)

Les dispositions de l'Annexe L de la Recommandation [UIT-T Y.4500.1] relatives à la procédure à suivre concernant l'actualisation et la tenue à jour des spécifications oneM2M s'appliquent à la présente Recommandation.

Bibliographie

[b-oneM2M TR-0008] oneM2M Technical Report TR-0008, *Security*.

[b-ATIS.oneM2M.TS0002V2.7.1] ATIS oneM2M.TS0002V2.7.1 (2016), *Requirements*. https://www.atis.org/docstore/product.aspx?id=28325

[b-ETSI TS 118 102] ETSI TS 118 102 v2.7.1 (2016), *oneM2M Requirements*. www.etsi.org/deliver/etsi_ts/118100_118199/118102/02.07.01_60/ts_118102v020701p.pdf

[b-TTA.oneM2M.TS0002V2.7.1] TTC oneM2M.TS0002V271 (2016), *Requirements*. http://www.tta.or.kr/data/ttas_view.jsp?rn=1&rn1=Y&rn2=&rn3=&nowpage=1&pk_num=TTAT.MMTS.0002+v2.7.1&standard_no=TTAT.MMTS.0002+v2.7.1&kor_standard=&publish_date=&section_code=&order=publish_date&by=desc&nowSu=1&totalSu=1&acode1=&acode2=&scode1=&scode2=

[b-TTC.oneM2M.TS0002V2.7.1] TTC oneM2M.TS0002V271 (2016), *Requirements*. www.ttc.or.jp/jp/document_list/pdf/j/TS/TS-M2M-0002v2.7.1.pdf

SÉRIES DES RECOMMANDATIONS UIT-T

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

Imprimé en Suisse
Genève, 2018